2018

Continued fractions and their applications

Joseph Tonien
University of Wollongong

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Continued Fractions and Their Applications

Joseph Tonien

Supervisors:
Associate Professor Peter Nickolas
Professor Martin Bunder

This thesis is presented as part of the requirements for the conferral of the degree:

Doctor of Philosophy

The University of Wollongong

School of Mathematics and Applied Statistics

February 2018

Declaration

I, Joseph Tonien, declare that this thesis submitted in partial fulfilment of the requirements for the conferral of the degree Doctor of Philosophy, from the University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. This document has not been submitted for qualifications at any other academic institution.

Joseph Tonien

Abstract

In this thesis, a special representation of numbers called *continued fraction* is studied. The continued fraction has a rich history and it is one of the most striking and powerful representations of numbers. For irrational numbers, a continued fraction expansion often reveals beautiful number patterns which remain obscured in their decimal expansion.

For the first part of this thesis, we prove some old and new continued fraction identities. Most of the proofs here are direct and elementary, where we use the Euler-Wallis recursive formula to derive closed form formulas for the convergents of particular continued fractions. A major part of the thesis is devoted to the study of the harmonic continued fraction and we determine the explicit convergence value for the even case of the harmonic continued fraction.

In the second part of the thesis, we show how to use continued fractions to develop efficient algorithms that can break public-key cryptosystems. Public-key cryptosystems are the backbone of Internet secure communication. We show that in the RSA cryptosystem and three other RSA-variant systems, if the keys are smaller than a certain bound, then it is possible to use continued fractions to determine the secret key from the public information.

Acknowledgements

I would like to thank my God, who created me and showed me a gleam of His beauty in the form of mathematics. I, a particle of His creation, would like to praise Him for His infinite mercy and goodness.

I am grateful to my supervisor, Professor Martin Bunder, who out of his kind heart, has provided me with enormous support during my University studies and my life in general. Professor Martin Bunder and his wife Simonette are my Godparents. With their grace and generosity, Martin and Simonette have been an inspiration and role model for me and my family.

I would like to thank my principal supervisor, A/Professor Peter Nickolas, for his valuable advice and guidance. I met Peter first time in 1997 at the University of Wollongong on the enrolment day of my Bachelor of Mathematics. During my undergraduate years, Peter taught me so many wonderful things – discrete mathematics, analysis, topology, wavelets – and now he has guided me completing my PhD thesis.

I would like to express my gratitude to Dr. James Borger for his encouragement and continued support. So many times, his kind words gave me the courage to continue.

A big thanks to Professor Willy Susilo for his friendship and mentoring. As the Head of the School of Computing and Information Technology, Willy has given me an excellent environment for conducting my research.

Finally, a special thanks to my family, my beloved wife Cậy and my five wonderful children Matthew, James, Francis, Vianney and Maryanna, you are my constant reminder of what a blessed person I truly am.

List of candidate's relevant publications

1. J. Tonien, A simple proof of Euler's continued fraction of $e^{1/M}$, *The Mathematical Gazette*, 100(548)(2016), 279–287.

2. M. Bunder and J. Tonien, *A new improved attack on RSA*, Proceedings of the 5th International Cryptology and Information Security Conference, 2016, 101-110.

3. M. Bunder, A. Nitaj, W. Susilo and J. Tonien, *A new attack on three variants of the RSA cryptosystem*, Proceedings of the 21st Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science 9723, 2016, 258–268.

4. M. Bunder and J. Tonien, A new attack on the RSA cryptosystem based on continued fractions, *Malaysian Journal of Mathematical Sciences*, 11(S3)(August 2017), 45–57.

5. J. Tonien, A continued fraction inspired by an identity of Euler, *The Mathematical Gazette*, 101(550)(2017), 115–121.

6. M. Bunder and J. Tonien, Closed form expressions for two harmonic continued fractions, *The Mathematical Gazette*, 101(552)(2017), 439–448.

7. M. Bunder, A. Nitaj, W. Susilo and J. Tonien, A generalized attack on RSA type cryptosystems, *Theoretical Computer Science*, 704(2017), 74–81.

8. J. Tonien, A new elementary proof of Euler's continued fractions, *The Mathematical Gazette*, 102(553)(2018), 105–111.

9. M. Bunder, P. Nickolas and J. Tonien, *On the harmonic continued fractions*, submitted.

Contents

Chapter 1

Introduction

1.1 Research aims

In this thesis, a special representation of numbers called "continued fraction" is studied. A continued fraction is an expression of the form

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots}}}$$

The continued fraction has a rich history and it is one of the most striking and powerful representations of numbers. Sometimes, numbers whose decimal expansions look totally random are revealed to have beautiful symmetries and patterns embedded deep within them when unfolded into a continued fraction.

Below are some beautiful continued fraction representations of the constant π:

$$\pi = \cfrac{4}{1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \ddots}}}}} = \cfrac{4}{1 + \cfrac{1^2}{3 + \cfrac{2^2}{5 + \cfrac{3^2}{7 + \cfrac{4^2}{\ddots}}}}} = 3 + \cfrac{1^2}{6 + \cfrac{3^2}{6 + \cfrac{5^2}{6 + \cfrac{7^2}{6 + \cfrac{9^2}{\ddots}}}}}$$

$$= 2+\cfrac{2}{\frac{1}{1}+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\frac{1}{4}+\cfrac{1}{\ddots}}}}} = 2+\cfrac{2}{1+\cfrac{1\times 2}{1+\cfrac{2\times 3}{1+\cfrac{3\times 4}{1+\cfrac{4\times 5}{1+\ddots}}}}} = 2+\cfrac{4}{3+\cfrac{1\times 3}{4+\cfrac{3\times 5}{4+\cfrac{5\times 7}{4+\cfrac{7\times 9}{4+\ddots}}}}}$$

This research has the following two main goals.

1. *To study classical results and develop further the theory of continued fractions.*

   There are numerous beautiful continued fractions developed by Euler, Lagrange, Gauss, Stieltjes, Ramanujan, ... using various methods. This research looks for alternative techniques which can be used to establish some of these classical results. For instance, we want to know if it is possible to find closed form formula for some of these continued fractions' convergents, or if it is possible to generalise some of these continued fractions.

2. *To find new applications of continued fractions.*

   Continued fractions have many applications. They are used in analysing Frieze patterns [17], in Rødseth's formula for Frobenius numbers [44], in computing the Jacobi symbol [2], in stream ciphers [24], in pseudo-random number generators [4], in cryptanalysis of the RSA public-key cryptosystem with small private exponents [5], [46]. This research looks for new applications of continued fractions in Computer Science.

1.2 Contributions and structure of thesis

In section 1.4, we review some fundamental results in the theory of continued fractions. These results are not new and can be found in most textbooks on number theory such as [6], [7], [21], [23], [25], [33].

Chapter 2 is based on the paper [41]. In this chapter, we present a proof of the following well-known continued fraction of $e^{1/M}$ due to Euler, that for any positive

real number M:

$$e^{1/M} = 1 + \cfrac{1}{M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{5M - 1 + \cfrac{1}{\ddots}}}}}}}}$$

Our proof is based on the following new continued fraction of $e^{1/M}$:

$$e^{1/M} = 1 + \cfrac{1}{M - \frac{1}{2} + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{7M + \cfrac{\frac{1}{4}}{\ddots}}}}}$$

Chapter 3 is based on the paper [43]. In this chapter, we present a new proof by contradiction of the following two continued fractions of the Euler's constant e:

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{\ddots}}}} = 2 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{4 + \cfrac{5}{\ddots}}}}$$

As a by-product, we obtain the following two new continued fractions

$$n+\cfrac{n}{n+1+\cfrac{n+1}{n+2+\cfrac{n+2}{n+3+\cfrac{n+3}{\ddots}}}}=-\frac{n}{n+1}\times\frac{e\sum_{k=0}^{n}\frac{(-1)^k}{k!}-1}{e\sum_{k=0}^{n+1}\frac{(-1)^k}{k!}-1},$$

and

$$n+\cfrac{n+1}{n+1+\cfrac{n+2}{n+2+\cfrac{n+3}{\ddots}}}=-\frac{e\sum_{k=0}^{n-1}\frac{(-1)^k}{k!}-1}{e\sum_{k=0}^{n}\frac{(-1)^k}{k!}-1}.$$

Chapter 4 is based on the paper [42]. In this chapter, we prove the following new continued fractions

$$a+1-\cfrac{1(a+1)}{a+3-\cfrac{2(a+2)}{a+5-\cfrac{3(a+3)}{\ddots\quad a+2n-1-\cfrac{n(a+n)}{a+2n+1}}}}$$

$$=\begin{cases}\dfrac{1}{\sum_{k=0}^{n}\frac{1}{k+1}} & \text{if } a=0\\[2ex] \dfrac{a}{1-\frac{(n+1)!}{(a+1)(a+2)\dots(a+n+1)}} & \text{if } a\neq 0\end{cases}$$

and

$$a+1-\cfrac{1(a+1)}{a+3-\cfrac{2(a+2)}{a+5-\cfrac{3(a+3)}{a+7-\cfrac{4(a+4)}{\ddots}}}}=\begin{cases}a & \text{if } a\geq 0\\ \\ 0 & \text{if } a<0 \text{ and } a\notin\mathbb{Z}\end{cases}$$

Chapter 5 is based on the paper [12]. In this chapter, we present a new proof of the following two continued fractions

$$\cfrac{1}{1}+\cfrac{1}{\cfrac{1}{2}+\cfrac{1}{\cfrac{1}{3}+\cfrac{1}{\cfrac{1}{4}+\cfrac{1}{\ddots}}}}=\frac{2}{\pi-2}$$

and

$$\cfrac{2}{1}+\cfrac{1}{\cfrac{2}{2}+\cfrac{1}{\cfrac{2}{3}+\cfrac{1}{\cfrac{2}{4}+\cfrac{1}{\ddots}}}}=\frac{1}{2\ln 2-1}.$$

As a by-product, we obtain the following new continued fractions

$$\cfrac{1}{1}+\cfrac{1}{\cfrac{1}{2}+\cfrac{1}{\cfrac{1}{3}+\cfrac{1}{\ddots+\cfrac{1}{\cfrac{1}{2n-1}}}}}=\cfrac{1}{\cfrac{1}{2n}\,\cfrac{2^2 4^2\ldots(2n)^2}{1^2 3^2\ldots(2n-1)^2}-1},$$

$$\frac{1}{1}+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{1}{2n}}}}}=\cfrac{1}{\frac{1}{2n+1}\,\frac{2^2 4^2\ldots(2n)^2}{1^2 3^2\ldots(2n-1)^2}-1},$$

$$\frac{2}{1}+\cfrac{1}{\frac{2}{2}+\cfrac{1}{\frac{2}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{2}{n}}}}}=\cfrac{1}{\sum\limits_{i=0}^{n-1}\frac{(-1)^i}{(i+1)(i+2)}}.$$

Chapter 6 is based on the paper [8] which is currently submitted for publication. In this chapter, we consider the *harmonic continued fraction*

$$HCF(t)=\frac{t}{1}+\cfrac{1}{\frac{t}{2}+\cfrac{1}{\frac{t}{3}+\cfrac{1}{\ddots}}},$$

for a general value of $t\in\mathbb{R}^+$.

We derive explicit formulas for the numerator and the denominator of the convergents. In particular, when $t=2a$ is an even positive integer, we can determine the exact value of $HCF(t)$:

$$HCF(2a)=\frac{(-1)^{a-1}}{2a\,\ln 2-1-2a\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{2\lfloor\frac{a}{2}\rfloor}\right)}.$$

In order to establish this result, we define and study the following *convolution alternating power sums*

$$T_{i,j}(n)=\sum_{k=0}^{n}(-1)^k k^i(n-k)^j$$

and prove some identities involving Euler polynomials and Stirling numbers, which are of independent interest.

The last two chapters are devoted to the application of continued fractions in cryp-

tography. We show how to use continued fractions to develop efficient algorithms that can break public-key cryptosystems. In a public-key cryptosystem, the encryption key and decryption key are different: the first one is made public and shared with everyone, whereas the latter one must be kept secret. Anyone can use the public key to encrypt a plaintext into a scrambled ciphertext but only the owner of the private key can decrypt the ciphertext back to the plaintext. Public-key cryptosystems are the backbone of Internet secure communication.

The public key and the private key are mathematically linked and it should be computationally impossible for anyone to determine the private key from the public key. This means that the system needs to be based on some hard computational maths problem. The RSA cryptosystem is based on the hardness of factorization of big numbers. To generate an RSA key, one would select two large prime numbers p and q, and multiply them to get a huge number $N = pq$. Next, choose two numbers $1 < e, d < (p-1)(q-1)$ such that $ed = 1 \pmod{(p-1)(q-1)}$. The public key is (N, e) and the private key is (p, q, d). A plaintext $1 < m < N$ is encrypted as $c = m^e \pmod{N}$ and the ciphertext c is decrypted as $m = c^d \pmod{N}$. The decryption and encryption cancel out each other thanks to Euler's theorem:

$$m^{(p-1)(q-1)} = 1 \pmod{N}.$$

The security of RSA system is based on the hardness of factorization of big numbers. Given a huge modulus N in the public key, say 2^{1000}, there is no efficient algorithm currently available to factor N to find out the two primes p and q. Thus, everyone knows N but no one knows $\phi(N) = (p-1)(q-1)$ except the owner of the key. So from the public information (N, e), it would be computationally impossible for anyone to determine the secret value $d = e^{-1} \pmod{\phi(N)}$.

We show that in the RSA cryptosystem and three other RSA-variant systems, if the keys are smaller than a certain bound then it is possible to use continued fractions to determine the secret key from the public information.

Chapter 7 is an extension of the papers [10], [11]. In this chapter, we will present an attack on the RSA cryptosystem. We show that, for an arbitrary parameter $t \in \mathbb{Z}^+$, if the public key (N, e) and the private key (p, q, d) satisfy

$$d^2 e < 8tN^{\frac{3}{2}},$$

then it is possible to efficiently perform the RSA number factorization and determine the private key using continued fractions, and the running time of our algorithm is $O(t \log N)$.

Our new attack is verified by an experiment with a 1024-bit modulus N and a 301-bit secret exponent d, which is out of reach for the previous attacks by Wiener [46] and Boneh et al [5].

Chapter 8 is an extension of the paper [9]. In this chapter, we apply the continued fraction method to launch a new attack on the three RSA-variant cryptosystems:

- The Kuwakado-Koyama-Tsuruoka scheme [28]: a scheme based on singular cubic curves $y^2 = x^3 + bx^2 \pmod N$ where $N = pq$ is an RSA modulus.
- The Elkamchouchi-Elshenawy-Shaban scheme [18]: an extension of the RSA scheme over the domain of Gaussian integers.
- The Castagnos scheme [13]: a public-key cryptosystem based on certain Lucas sequences.

We show that, for an arbitrary parameter $t \in \mathbb{Z}^+$, if the public key (N, e) and the private key (p, q, d) satisfy

$$d^2 e < 2t\frac{(N^2 - \frac{5}{2}N)^2}{N + 4t} \approx 2tN^3,$$

then there is an algorithm with running time $O(t \log N)$ that can determine the private key from the public key. Our new attack is verified by an experiment with a 1024-bit modulus N, a 2029-bit public key e and a 520-bit private key d.

1.3 Future work

A major work in the first part of this thesis is to investigate the harmonic continued fraction $HCF(t)$. In chapter 5, we give a simple and direct proof of closed form formulas for $HCF(1)$ and $HCF(2)$. In chapter 6, we give a closed form formula for the even case, $HCF(2a)$ for all positive integer a. It is our future work to determine a closed form formula for the odd case, $HCF(2a + 1)$, and the general case, $HCF(t)$, for all positive real number t. It is also our future work to look at the rate of convergence of these continued fractions as the value of t varies.

The second part of the thesis looks at the applications of continued fractions in cryptography, particularly in public key encryption algorithms, RSA and variants of RSA. It is our future work to look at other applications in cryptography, such as pseudo-random generator and stream ciphers.

1.4 Preliminaries

In this section, we review some fundamental results in the theory of continued fractions. These results are not new and can be found in most textbooks on number theory such as [6], [7], [21], [23], [25], [33].

1.4.1 The convergents of a continued fraction

Throughout this thesis, we will use the following notations

$$[a_0, (b_0, a_1), (b_1, a_2), \dots] = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots}}},$$

$$[a_0, (b_0, a_1), \dots, (b_{n-1}, a_n)] = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{\ddots\, a_{n-1} + \cfrac{b_{n-1}}{a_n}}}.$$

The truncated continued fraction $[a_0, (b_0, a_1), \dots, (b_{n-1}, a_n)]$ is called the n^{th} *convergent* of the longer continued fraction $[a_0, (b_0, a_1), \dots, (b_{n-1}, a_n), \dots]$

An *ordinary continued fraction* is a continued fraction with all the b_i coefficients equal to 1. We will use the following shorter notations to denote ordinary continued fractions:

$$[a_0, a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

$$[a_0, a_1, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}.$$

In this case, the truncated continued fraction $[a_0, a_1, \dots, a_n]$ is the n^{th} *convergent* of the longer continued fraction $[a_0, a_1, a_2, \dots]$.

The value of a finite continued fraction is clearly determined. The value of an infinite continued fraction is defined in a natural way:

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots}}} = \lim_{n\to\infty} [a_0, (b_0, a_1), \ldots, (b_{n-1}, a_n)].$$

If this limit exists then we say that the infinite continued fraction *converges*.

1.4.2 The Euler-Wallis recursive formula

To prove that a continued fraction converges, we often need to determine its convergent sequence. The following theorem due to William Brouncker (1620-1684), the first President of the Royal Society, gives us recursive formulas to calculate the convergents. John Wallis (1616-1703) and Leonhard Euler (1707-1783) made extensive use of these formulas, which are now called the Euler-Wallis formulas.

Theorem 1.4.1 *[45]. For any $n \geq 0$, the n^{th} convergent can be determined as*

$$c_n = \frac{p_n}{q_n},$$

where the numerator and the denominator sequences $\{p_n\}_{n\geq -2}$ and $\{q_n\}_{n\geq -2}$ are specified as follows (with the convention that $b_{-1} = 1$):

$$p_{-2} = 0, \quad p_{-1} = 1, \quad p_n = a_n p_{n-1} + b_{n-1} p_{n-2}, \ \forall n \geq 0,$$

$$q_{-2} = 1, \quad q_{-1} = 0, \quad q_n = a_n q_{n-1} + b_{n-1} q_{n-2}, \ \forall n \geq 0.$$

Proof. We prove this by induction. In the base case $n = 0$, we have $p_0 = a_0$ and $q_0 = 1$, so the formulas are correct. To prove the $n + 1$ case, modify the coefficient a_n to be $a_n + \frac{b_n}{a_{n+1}}$, the $(n+1)^{\text{th}}$ convergent is equal to the modified n^{th} convergent, and thus by the induction hypothesis,

$$\begin{aligned}\frac{p_{n+1}}{q_{n+1}} &= \frac{\left(a_n + \frac{b_n}{a_{n+1}}\right) p_{n-1} + b_{n-1} p_{n-2}}{\left(a_n + \frac{b_n}{a_{n+1}}\right) q_{n-1} + b_{n-1} q_{n-2}} = \frac{a_{n+1}(a_n p_{n-1} + b_{n-1} p_{n-2}) + b_n p_{n-1}}{a_{n+1}(a_n q_{n-1} + b_{n-1} q_{n-2}) + b_n q_{n-1}} \\ &= \frac{a_{n+1} p_n + b_n p_{n-1}}{a_{n+1} q_n + b_n q_{n-1}}.\end{aligned}$$

This completes the proof. ■

Note that the convergents start with $c_0 = p_0/q_0$, but allowing the recursive formulas to hold for $n = 0$ and $n = 1$, in Theorem 1.4.1, we extend the sequence index to $n = -1$ and $n = -2$ and also make the convention that $b_{-1} = 1$.

Sometimes we want to investigate the sub-sequences $\{p_{2n}\}$, $\{p_{2n-1}\}$, $\{q_{2n}\}$, $\{q_{2n-1}\}$ and the following theorem is useful in those scenarios.

Theorem 1.4.2 *The convergents $\frac{p_n}{q_n}$ satisfy the following:*

$$p_n = \left(a_n a_{n-1} + \frac{a_n b_{n-2}}{a_{n-2}} + b_{n-1}\right)\ p_{n-2} - \frac{a_n b_{n-2} b_{n-3}}{a_{n-2}}\ p_{n-4}, \quad \forall n \geq 2,$$
$$q_n = \left(a_n a_{n-1} + \frac{a_n b_{n-2}}{a_{n-2}} + b_{n-1}\right)\ q_{n-2} - \frac{a_n b_{n-2} b_{n-3}}{a_{n-2}}\ q_{n-4}, \quad \forall n \geq 2.$$

Proof. By the Euler-Wallis formula,

$$p_{n-2} = a_{n-2}\ p_{n-3} + b_{n-3}\ p_{n-4},\ \forall n \geq 2,$$

so

$$p_{n-3} = \frac{1}{a_{n-2}}\ p_{n-2} - \frac{b_{n-3}}{a_{n-2}}\ p_{n-4}.$$

Using the Euler-Wallis formula again, we have

$$\begin{aligned} p_{n-1} &= a_{n-1}\ p_{n-2} + b_{n-2}\ p_{n-3} \\ &= a_{n-1}\ p_{n-2} + b_{n-2}\ \left(\frac{1}{a_{n-2}}\ p_{n-2} - \frac{b_{n-3}}{a_{n-2}}\ p_{n-4}\right) \\ &= \left(a_{n-1} + \frac{b_{n-2}}{a_{n-2}}\right) p_{n-2} - \frac{b_{n-2}\ b_{n-3}}{a_{n-2}} p_{n-4}. \end{aligned}$$

Finally, applying the Euler-Wallis formula once more, we have

$$\begin{aligned} p_n &= a_n\ p_{n-1} + b_{n-1}\ p_{n-2} \\ &= a_n \left(\left(a_{n-1} + \frac{b_{n-2}}{a_{n-2}}\right) p_{n-2} - \frac{b_{n-2}\ b_{n-3}}{a_{n-2}} p_{n-4}\right) + b_{n-1}\ p_{n-2} \\ &= \left(a_n a_{n-1} + \frac{a_n b_{n-2}}{a_{n-2}} + b_{n-1}\right)\ p_{n-2} - \frac{a_n b_{n-2} b_{n-3}}{a_{n-2}}\ p_{n-4}. \end{aligned}$$

The relation for q_n is proved similarly. ■

Using the Euler-Wallis recurrence formulas, it is easy to prove the following identities for convergents.

Theorem 1.4.3 *[25] The convergents satisfy the following identities:*

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1} \prod_{i=0}^{n-1} b_i, \quad \forall n \geq -1, \tag{1.1}$$

$$p_n q_{n-2} - q_n p_{n-2} = (-1)^n a_n \prod_{i=0}^{n-2} b_i, \quad \forall n \geq 0, \tag{1.2}$$

with the convention that $\prod_{i=0}^{-2} b_i = \prod_{i=0}^{-1} b_i = 1$.

Proof. The identity (1.1) is true for $n = -1$ and $n = 0$ as $p_{-1}q_{-2} - q_{-1}p_{-2} = 1$ and $p_0 q_{-1} - q_0 p_{-1} = -1$. For $n \geq 1$, it follows from the following equation:

$$\begin{aligned} p_n q_{n-1} - q_n p_{n-1} &= (a_n p_{n-1} + b_{n-1} p_{n-2}) q_{n-1} - (a_n q_{n-1} + b_{n-1} q_{n-2}) p_{n-1} \\ &= -b_{n-1}(p_{n-1} q_{n-2} - q_{n-1} p_{n-2}). \end{aligned}$$

The identity (1.2) is a consequence of the following equation and (1.1):

$$\begin{aligned} p_n q_{n-2} - q_n p_{n-2} &= (a_n p_{n-1} + b_{n-1} p_{n-2}) q_{n-2} - (a_n q_{n-1} + b_{n-1} q_{n-2}) p_{n-2} \\ &= a_n(p_{n-1} q_{n-2} - q_{n-1} p_{n-2}), \ \forall n \geq 0. \quad \blacksquare \end{aligned}$$

The following theorem is a direct consequence of Theorem 1.4.3.

Theorem 1.4.4 *The convergents of an* ordinary continued fraction *satisfy the following identities:*

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}, \quad \forall n \geq -1, \tag{1.3}$$

$$p_n q_{n-2} - q_n p_{n-2} = (-1)^n a_n, \quad \forall n \geq 0. \tag{1.4}$$

1.4.3 Convergence of continued fractions with positive coefficients

Theorem 1.4.5 *[25] If* $a_n > 0$ *for all* $n \geq 1$, $b_n > 0$ *for all* $n \geq 0$, *and*

$$\lim_{n \to \infty} \frac{b_0 b_1 \dots b_{2n}}{q_{2n} q_{2n+1}} = 0$$

then the continued fraction converges.

Proof. By the Euler-Wallis recursive formula, $q_n > 0$ for all $n \geq 0$. From the

identities of Theorem 1.4.3 we have

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1} b_0 b_1 \dots b_{n-1}}{q_{n-1} q_n},$$
$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^{n} a_n b_0 b_1 \dots b_{n-2}}{q_{n-2} q_n}.$$

It follows that,

$$\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \dots > \frac{p_{2n+1}}{q_{2n+1}} > \dots > \frac{p_{2n}}{q_{2n}} > \dots > \frac{p_4}{q_4} > \frac{p_2}{q_2} > \frac{p_0}{q_0}.$$

Thus, in this case the two sub-sequences $\{\frac{p_{2n}}{q_{2n}}\}$ and $\{\frac{p_{2n+1}}{q_{2n+1}}\}$ always converge, and the continued fraction converges if and only if

$$\lim_{n\to\infty} \left(\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} \right) = \lim_{n\to\infty} \frac{b_0 b_1 \dots b_{2n}}{q_{2n} q_{2n+1}} = 0. \quad \blacksquare$$

Theorem 1.4.6 *[25] If $a_n > 0$ for all $n \geq 1$, $b_n > 0$ for all $n \geq 0$, and*

$$\lim_{n\to\infty} \frac{b_0 b_1 \dots b_{2n}}{a_1^2 \dots a_{2n}^2 \; a_{2n+1}} = 0.$$

then the continued fraction converges.

Proof. Since $q_0 = 1$ and $q_n \geq a_n q_{n-1}$, we have $q_n \geq a_1 \dots a_n$ for all $n \geq 1$, and thus,

$$\frac{b_0 b_1 \dots b_{2n}}{q_{2n} q_{2n+1}} \leq \frac{b_0 b_1 \dots b_{2n}}{a_1^2 \dots a_{2n}^2 \; a_{2n+1}}.$$

Therefore, by Theorem 1.4.5, the continued fraction converges if

$$\lim_{n\to\infty} \frac{b_0 b_1 \dots b_{2n}}{a_1^2 \dots a_{2n}^2 \; a_{2n+1}} = 0. \quad \blacksquare$$

Theorem 1.4.7 *[25] If $a_n \geq 1$ for all $n \geq 1$, then the ordinary continued fraction $[a_0, a_1, a_2, a_3, \dots]$ converges.*

Proof. Since $q_0 = 1$, $q_1 = a_1 \geq 1$ and $q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2}$ for all $n \geq 2$, q_n tends to infinity. By Theorem 1.4.5, the continued fraction converges. $\blacksquare$

Theorem 1.4.7 is a special case of a more general theorem due to Seidel and Stern [3], [30], [38], [39], dating back to the 1840s:

Theorem 1.4.8 (The Seidel-Stern Theorem) *[25] If $a_n > 0$ for all $n \geq 1$ then the ordinary continued fraction $[a_0, a_1, a_2, a_3, \dots]$ converges if, and only if, $\sum_{n=0}^{\infty} a_n$ diverges.*

Proof. We have

$$q_{-1} = 0, \quad q_0 = 1, \quad q_n = a_n q_{n-1} + q_{n-2} > q_{n-2}, \quad \forall n \geq 1,$$

so the sequences $\{q_{2n}\}$ and $\{q_{2n+1}\}$ are increasing and

$$q_n \geq \min(q_0, q_1) > 0, \quad \forall n \geq 0.$$

We have

$$q_n - q_{n-2} = a_n q_{n-1} \geq \min(q_0, q_1)\ a_n, \quad \forall n \geq 1.$$

Taking summation, we obtain

$$q_n + q_{n-1} - q_0 - q_{-1} \geq \min(q_0, q_1)\ \sum_{i=1}^{n} a_i, \quad \forall n \geq 2,$$

and

$$q_n + q_{n-1} \geq q_0 + q_{-1} + \min(q_0, q_1)\ \sum_{i=1}^{n} a_i.$$

Therefore, if the series $\sum_i a_i$ diverges then $q_n + q_{n-1}$ tends to infinity, and as

$$\begin{aligned} q_n q_{n-1} &\geq q_n\ \min(q_0, q_1), \\ q_n q_{n-1} &\geq q_{n-1}\ \min(q_0, q_1), \\ 2q_n q_{n-1} &\geq (q_n + q_{n-1})\ \min(q_0, q_1), \end{aligned}$$

it follows that $q_n q_{n-1}$ also tends to infinity, by Theorem 1.4.5, the continued fraction converges.

Now suppose that $\sum_k a_k$ converges; we will show that the continued fraction diverges. By Theorem 1.4.5, it suffices to show that $\{q_n\}$ is bounded. We prove by induction that

$$q_n \leq e^{\sum_{i=1}^{n} a_i} \max(q_0, q_1).$$

Indeed,

$$\begin{aligned} q_0 &\leq \max(q_0, q_1), \\ q_1 &\leq \max(q_0, q_1) \leq e^{a_1} \max(q_0, q_1). \end{aligned}$$

At induction step, we have

$$\begin{aligned} q_n &= a_n q_{n-1} + q_{n-2} \\ &\le a_n \; e^{\sum_{i=1}^{n-1} a_i} \max(q_0, q_1) + e^{\sum_{i=1}^{n-2} a_i} \max(q_0, q_1) \\ &\le a_n \; e^{\sum_{i=1}^{n-1} a_i} \max(q_0, q_1) + e^{\sum_{i=1}^{n-1} a_i} \max(q_0, q_1) \\ &= (a_n + 1) \; e^{\sum_{i=1}^{n-1} a_i} \max(q_0, q_1) \\ &\le e^{a_n} \; e^{\sum_{i=1}^{n-1} a_i} \max(q_0, q_1) \\ &= e^{\sum_{i=1}^{n} a_i} \max(q_0, q_1). \end{aligned}$$

This completes the proof. ■

1.4.4 The Legendre theorem

An ordinary continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

is called a *regular continued fraction* if the coefficient a_0 is an integer and all the coefficients a_i for $i \ge 1$ are positive integers.

There is a standard way to generate a unique regular continued fraction from any real number and it is this continued fraction we refer to when we say *the continued fraction* of a real number. This continued fraction expansion of a number is formed by subtracting away the integer part of it and inverting the remainder, and then repeating this process again and again.

Definition 1.4.1 *For a given number $x \in \mathbb{R}$, a sequence $\{a_n\}_{n\ge 0}$ is uniquely determined as follows*

- $x_0 = x, \quad a_0 = \lfloor x_0 \rfloor,$
- *for each $n \ge 0$, if $x_n \in \mathbb{Z}$ then the process terminates, otherwise, define*

$$x_{n+1} = \frac{1}{x_n - a_n}, \quad a_{n+1} = \lfloor x_{n+1} \rfloor.$$

The sequence $\{a_n\}_{n\ge 0}$ is finite if $x \in \mathbb{Q}$ and infinite if $x \notin \mathbb{Q}$. The resulting regular continued fraction $[a_0, a_1, a_2, \dots]$ is called "the regular continued fraction" of x. The

convergents of the regular continued fraction of x are referred to as the convergents of x.

From the construction in Definition 1.4.1, we can see that

$$\begin{aligned} x = x_0 &= a_0 + (x_0 - a_0) = a_0 + \frac{1}{x_1} \text{ if } x_0 \notin \mathbb{Z} \\ &= a_0 + \frac{1}{a_1 + (x_1 - a_1)} = a_0 + \frac{1}{a_1 + \dfrac{1}{x_2}} \text{ if } x_1 \notin \mathbb{Z} \\ &= a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + (x_2 - a_2)}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \dfrac{1}{x_3}}} \text{ if } x_2 \notin \mathbb{Z} \\ &= \dots \end{aligned}$$

so

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_n + \cfrac{1}{x_{n+1}}}}. \tag{1.5}$$

For example,

$$\begin{aligned} \frac{1000}{987} &= 1 + \frac{13}{987} = 1 + \frac{1}{\frac{987}{13}} \\ &= 1 + \frac{1}{75 + \dfrac{12}{13}} = 1 + \frac{1}{75 + \frac{1}{\frac{13}{12}}} \\ &= 1 + \cfrac{1}{75 + \cfrac{1}{1 + \cfrac{1}{12}}}. \end{aligned}$$

The above process of constructing the continued fraction for $\frac{1000}{987}$ is the exact mirror

of the *Euclidean division algorithm*

$$\begin{aligned} 1000 &= 987 \times 1 + 13 \\ 987 &= 13 \times 75 + 12 \\ 13 &= 12 \times 1 + 1 \\ 12 &= 1 \times 12 + 0. \end{aligned}$$

Since the Euclidean division algorithm always terminates, the continued fraction of a rational number has a finite length. On the other hand, the continued fraction of an irrational number continues forever.

If $x \in \mathbb{Q}$ and the construction in Definition 1.4.1 terminates at n then

$$x = [a_0, a_1, \ldots, a_n],$$

and in this case, we have two regular continued fractions that equal x:

$$\begin{aligned} x &= [a_0, a_1, \ldots, a_n] \\ &= [a_0, a_1, \ldots, a_n - 1, 1], \end{aligned} \tag{1.6}$$

but the first one $[a_0, a_1, \ldots, a_n]$ is "the regular continued fraction" of x, whereas, the second one $[a_0, a_1, \ldots, a_n - 1, 1]$ is not.

If $x \notin \mathbb{Q}$, it follows from the equation (1.5) that

$$[a_0, a_1, \ldots, a_{2n}] < x < [a_0, a_1, \ldots, a_{2n+1}] \quad \forall n \geq 0.$$

Since every regular continued fraction converges by Theorem 1.4.7, *the regular continued fraction* $[a_0, a_1, \ldots]$ of x must converge to x.

Theorem 1.4.9 (The Legendre Theorem) *[29] Let $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$ such that*

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}.$$

Then $\frac{p}{q}$ is equal to a convergent of the regular continued fraction of x.

Proof. If $x = \frac{p}{q}$ then $\frac{p}{q}$ is equal to the last convergent of x, so we assume that $x \neq \frac{p}{q}$. As noted above in (1.6), a rational number $\frac{p}{q}$ can be written as a regular continued fraction of even and as a regular continued fraction of odd length. So, we will write

$$\frac{p}{q} = [a_0, a_1, \ldots, a_n]$$

such that n is even if $x > \frac{p}{q}$ and n is odd in the case $x < \frac{p}{q}$. Define $sign(z)$ to be 1, -1, or 0 if z is positive, negative or zero, respectively; then

$$sign(x - \frac{p}{q}) = (-1)^n.$$

If we define a by

$$x = [a_0, a_1, \ldots, a_n, a], \tag{1.7}$$

the theorem is proved if we can show that $a > 1$.

Since

$$\frac{p}{q} = [a_0, a_1, \ldots, a_n],$$
$$x = [a_0, a_1, \ldots, a_n, a],$$

by the Euler-Wallis recursive formula,

$$\frac{p}{q} = \frac{p_n}{q_n},$$
$$x = \frac{p_{n+1}}{q_{n+1}} = \frac{ap_n + p_{n-1}}{aq_n + q_{n-1}},$$

so

$$x - \frac{p}{q} = \frac{ap_n + p_{n-1}}{aq_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(aq_n + q_{n-1})}.$$

By Theorem 1.4.4,

$$x - \frac{p}{q} = \frac{(-1)^n}{q_n(aq_n + q_{n-1})} = \frac{sign(x - \frac{p}{q})}{q_n(aq_n + q_{n-1})}.$$

Therefore,

$$\left| x - \frac{p}{q} \right| = \frac{1}{q_n(aq_n + q_{n-1})}.$$

The hypothesis

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$$

implies

$$q_n(aq_n + q_{n-1}) > 2q^2. \tag{1.8}$$

Since $\gcd(p_n, q_n) = 1$ by Theorem 1.4.4 and $\frac{p}{q} = \frac{p_n}{q_n}$, we have $q \geq q_n$. We also have $q_n \geq q_{n-1}$, so it follows from (1.8) that $a > 1$, and the proof is completed. ■

Chapter 2

Continued Fraction Expansions of $e^{1/M}$

In this chapter, we will present a proof of the following continued fraction of $e^{1/M}$ due to Euler, that for any positive real number M:

$$e^{1/M} = 1 + \cfrac{1}{M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{5M - 1 + \cfrac{1}{\ddots}}}}}}}} \tag{2.1}$$

Our proof contains two steps. In the first step, we show that

$$e^{1/M} = 1 + \cfrac{1}{M - \frac{1}{2} + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{7M + \cfrac{\frac{1}{4}}{\ddots}}}}} \tag{2.2}$$

And in the second step of the proof, we use the algebraic identity

$$(2k+1)M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{x}}} = (2k+1)M - \frac{1}{2} + \frac{\frac{1}{4}}{\frac{1}{2} + x}$$

to transform the continued fraction (2.2) into the form (2.1).

In a foundational publication on the theory of continued fractions, *"De Fractionibus Continuis Dissertatio"* [19], Euler used the Ricatti differential equation to derive the continued fraction (2.1). This continued fraction (2.1) can also be obtained from a continued fraction of the function $\tanh z$ using the Hurwitz transformation (see exercises 14 and 16, section 4.5.3 of [27]). When $M = 1$, we have the following regular continued fraction expansion of e

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{8 + \ddots}}}}}}}}}}} \tag{2.3}$$

Since a rational number must have a finite regular continued fraction expansion, this implies that e is irrational. Lagrange's theorem [33] asserts that a real number has a periodic regular continued fraction if and only if it is a quadratic irrational. Since (2.3) is not periodic, e must not be algebraic of degree 2.

Using integration of the form $\int e^{-rx} x^n (1-x)^n dx$, Hermite [22] gave the first proof that e is transcendental. As a by-product, Hermite also derived the identity (2.3). Based on Hermite's work, Olds [34] gave an expository proof of the continued fraction of e. Cohn [15] streamlined Olds' proof into a short presentation. Osler [35] extended

Cohn's proof to the general case of $e^{1/M}$. All of these proofs rely heavily on the integration technique.

Here we will present a simple proof of the identity (2.1), which only involves the manipulation of recurrence equations.

This chapter is based on the paper [41].

2.1 A new continued fraction expansion of $e^{1/M}$

This is the first step of the proof. We will prove the following new continued fraction

$$M+\cfrac{\frac{1}{4}}{3M+\cfrac{\frac{1}{4}}{5M+\cfrac{\frac{1}{4}}{7M+\cfrac{\frac{1}{4}}{\ddots}}}}=\frac{1}{e^{1/M}-1}+\frac{1}{2} \tag{2.4}$$

which gives rise to a new continued fraction expansion of $e^{1/M}$

$$e^{1/M}=1+\cfrac{1}{M-\frac{1}{2}+\cfrac{\frac{1}{4}}{3M+\cfrac{\frac{1}{4}}{5M+\cfrac{\frac{1}{4}}{7M+\cfrac{\frac{1}{4}}{\ddots}}}}}$$

Lemma 2.1.1 *For a positive real number M, let*

$$\begin{aligned}
S_0 &= \sum_{i=1}^{\infty} \frac{1}{i!M^i} \\
S_1 &= \sum_{i=1}^{\infty} \frac{i-1}{(i+1)!M^i} \\
&\vdots \\
S_k &= \sum_{i=1}^{\infty} \frac{(i-1)(i-2)\dots(i-k)}{(i+k)!M^i}
\end{aligned}$$

then

$$S_{n+2}+(4n+6)MS_{n+1}-S_n=0. \tag{2.5}$$

Proof. $S_0 = e^{1/M} - 1$, and by the ratio test, we can see that each of the series S_k converges to a positive number. We have

$$\begin{aligned}
&S_n - (4n+6)MS_{n+1} \\
&= \sum_{i=1}^{\infty} \frac{(i-1)(i-2)\dots(i-n)}{(i+n)!M^i} - (4n+6)\sum_{i=1}^{\infty} \frac{(i-1)(i-2)\dots(i-n-1)}{(i+n+1)!M^{i-1}} \\
&= \sum_{i=1}^{\infty} \frac{(i-1)(i-2)\dots(i-n)}{(i+n)!M^i} - (4n+6)\sum_{i=1}^{\infty} \frac{i(i-1)\dots(i-n)}{(i+n+2)!M^i} \\
&= \sum_{i=1}^{\infty} \frac{(i-1)(i-2)\dots(i-n)[(i+n+1)(i+n+2) - (4n+6)i]}{(i+n+2)!M^i} \\
&= \sum_{i=1}^{\infty} \frac{(i-1)(i-2)\dots(i-n)(i-n-1)(i-n-2)}{(i+n+2)!M^i} \\
&= S_{n+2}. \quad \blacksquare
\end{aligned}$$

We want to make the recurrence relation (2.5) hold for $n = -1$, so we define S_{-1} as follows:

$$\begin{aligned}
S_{-1} &= S_1 + 2MS_0 \\
&= \sum_{i=1}^{\infty} \frac{i-1}{(i+1)!M^i} + 2M\sum_{i=1}^{\infty} \frac{1}{i!M^i} \\
&= 2 + \sum_{i=1}^{\infty} \frac{i-1}{(i+1)!M^i} + 2\sum_{i=2}^{\infty} \frac{1}{i!M^{i-1}} \\
&= 2 + \sum_{i=1}^{\infty} \frac{i-1}{(i+1)!M^i} + 2\sum_{i=1}^{\infty} \frac{1}{(i+1)!M^i} \\
&= 2 + \sum_{i=1}^{\infty} \frac{i+1}{(i+1)!M^i} = 2 + \sum_{i=1}^{\infty} \frac{1}{i!M^i} \\
&= e^{1/M} + 1.
\end{aligned}$$

Now we have

$$S_{n+2} + (4n+6)MS_{n+1} - S_n = 0, \quad \forall n \geq -1,$$

and we will use this recurrence relation to establish a finite continued fraction which looks like (2.4).

Lemma 2.1.2 *Using the sequence $\{S_n\}$ of Lemma 2.1.1, for any $n \geq 0$,*

$$M + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{\ddots\,(2n+1)M + \cfrac{\frac{1}{4}}{\frac{S_n}{2S_{n+1}}}}}} = \frac{1}{e^{1/M}-1} + \frac{1}{2}.$$

Proof. Since

$$S_{n+2} + (4n+6)MS_{n+1} - S_n = 0$$

we have

$$\frac{S_n}{2S_{n+1}} = (2n+3)M + \frac{S_{n+2}}{2S_{n+1}}$$

and

$$\frac{S_n}{2S_{n+1}} = (2n+3)M + \frac{\frac{1}{4}}{\frac{S_{n+1}}{2S_{n+2}}}.$$

So for any $n \geq 0$,

$$\begin{aligned}
\frac{1}{e^{1/M}-1} + \frac{1}{2} &= \frac{e^{1/M}+1}{2(e^{1/M}-1)} \\
&= \frac{S_{-1}}{2S_0} \\
&= M + \frac{\frac{1}{4}}{\frac{S_0}{2S_1}} \\
&= M + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{\frac{S_1}{2S_2}}} \\
&= M + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{\frac{S_2}{2S_3}}}} = \dots \\
&= M + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{\ddots\,(2n+1)M + \cfrac{\frac{1}{4}}{\frac{S_n}{2S_{n+1}}}}}}.
\end{aligned}$$

■

Lemma 2.1.2 almost gives us the continued fraction (2.4). Does Lemma 2.1.2 immediately imply that the infinite continued fraction

$$[M, (\frac{1}{4}, 3M), (\frac{1}{4}, 5M), \dots]$$

converges to $\frac{1}{e^{1/M}-1} + \frac{1}{2}$?

Here is an example. Since $x_0 = 1 - \sqrt{2}$ is a root of the quadratic equation

$$x^2 - 2x - 1 = 0,$$

we have $x_0 = 2 + \frac{1}{x_0}$. This gives us the following continued fraction of arbitrary length

$$1 - \sqrt{2} = 2 + \cfrac{1}{2 + \cfrac{1}{\ddots\ 2 + \cfrac{1}{2 + (-1 - \sqrt{2})}}}$$

Does this mean the infinite continued fraction $[2, (1, 2), (1, 2), \dots]$ converges to the value $1 - \sqrt{2}$? No, in fact, this continued fraction converges to $1 + \sqrt{2}$.

The difference between Lemma 2.1.2 and the above "$1 - \sqrt{2}$ example" is that in Lemma 2.1.2, the "trailing part" $\frac{S_n}{2S_{n+1}}$ is positive, whereas in the "$1 - \sqrt{2}$ example", the "trailing part" $(-1 - \sqrt{2})$ is negative. Because $\frac{S_n}{2S_{n+1}}$ is positive, we can use Lemma 2.1.2 to find the convergence value of the infinite continued fraction using the Markov test which appears in the following theorem.

Theorem 2.1.1 *[26] Suppose that the coefficients a_n, b_n are all positive and that the infinite continued fraction converges:*

$$[a_0, (b_0, a_1), (b_1, a_2), \dots] = \ell.$$

Construct a sequence $\{z_n\}$ such that

$$z_0 = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{\ddots\ a_{n-1} + \cfrac{b_{n-1}}{a_n + z_n}}}$$

In this construction, if z_n are all positive then z_0 must be equal to ℓ.

Proof. Let $\tau_0(x) = a_0 + x$, $\tau_k(x) = b_{k-1}/(a_k + x)$ then

$$z_0 = T_n(z_n) = \tau_0 \circ \tau_1 \circ \cdots \circ \tau_n(z_n)$$

Every function τ_k is continuous and monotonic on $[0, +\infty)$. Hence the same is true for their composition T_n. Picking two limit values $x = 0$ and $x = +\infty$, we obtain that z_0 must be in the interval with the end-points at

$$T_n(0) = \frac{p_n}{q_n}, \qquad T_n(+\infty) = \frac{p_{n-1}}{q_{n-1}}$$

Since the continued fraction is assumed to converge to ℓ, we have $z_0 = \ell$. ■

Theorem 2.1.2 *For any positive real number M,*

$$M + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{7M + \cfrac{\frac{1}{4}}{\ddots}}}} = \frac{1}{e^{1/M} - 1} + \frac{1}{2}.$$

Proof. The convergence is obtained from Theorem 1.4.6. By the Markov convergence test (Theorem 2.1.1), Lemma 2.1.2 implies that the infinite continued fraction does converge to $\frac{1}{e^{1/M}-1} + \frac{1}{2}$. ■

By Theorem 2.1.2, we obtain the following continued fraction expansion of $e^{1/M}$

$$e^{1/M} = 1 + \cfrac{1}{M - \frac{1}{2} + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{7M + \cfrac{\frac{1}{4}}{\ddots}}}}}$$

and this completes the first step of the proof.

2.2 A proof of the Euler continued fraction

In the second step of the proof, we will use the following algebraic identity

$$(2k+1)M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{x}}} = (2k+1)M - \frac{1}{2} + \frac{\frac{1}{4}}{\frac{1}{2} + x} \tag{2.6}$$

to transform the previous continued fraction into the following Euler continued fraction.

Theorem 2.2.1 *For any positive real number M,*

$$e^{1/M} = 1 + \cfrac{1}{M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3M - 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{5M - 1 + \cfrac{1}{\ddots}}}}}}}}$$

Proof. The coefficients of this continued fraction are eventually positive, and by Theorem 1.4.6, the continued fraction converges.

We apply the identity (2.6) repeatedly as follows

$$
\begin{aligned}
&1+\cfrac{1}{\mathbf{M-1}+\cfrac{1}{\mathbf{1}+\cfrac{1}{\mathbf{1}+\cfrac{1}{3M-1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{5M-1+\cfrac{1}{\ddots}}}}}}}}}\\
&=1+\cfrac{1}{M-\frac{1}{2}+\cfrac{\frac{1}{4}}{\frac{1}{2}+\mathbf{3M-1}+\cfrac{1}{\mathbf{1}+\cfrac{1}{\mathbf{1}+\cfrac{1}{5M-1+\cfrac{1}{\ddots}}}}}}\\
&=1+\cfrac{1}{M-\frac{1}{2}+\cfrac{\frac{1}{4}}{\frac{1}{2}+3M-\frac{1}{2}+\cfrac{\frac{1}{4}}{\frac{1}{2}+5M-1+\cfrac{1}{\ddots}}}}\\
&=\dots
\end{aligned}
$$

$$= 1 + \cfrac{1}{M - \frac{1}{2} + \cfrac{\frac{1}{4}}{\frac{1}{2} + 3M - \frac{1}{2} + \cfrac{\frac{1}{4}}{\frac{1}{2} + 5M - \frac{1}{2} + \cfrac{\frac{1}{4}}{\frac{1}{2} + 7M - \frac{1}{2} + \frac{\frac{1}{4}}{\ddots}}}}}}$$

$$= 1 + \cfrac{1}{M - \frac{1}{2} + \cfrac{\frac{1}{4}}{3M + \cfrac{\frac{1}{4}}{5M + \cfrac{\frac{1}{4}}{7M + \frac{\frac{1}{4}}{\ddots}}}}} = e^{1/M}. \quad \blacksquare$$

We have now proved the continued fraction expansion formula for $e^{1/M}$. $\blacksquare$

Chapter 3

Continued Fraction Expansions of e

In this chapter, we will present a new proof by contradiction of the following two continued fractions [20] of Euler's constant e:

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{\ddots}}}} = 2 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{4 + \cfrac{5}{\ddots}}}} \tag{3.1}$$

For the first identity, suppose that the continued fraction converges to x, then we will determine a closed form formula for its subfraction as follows:

$$u_n = n + \cfrac{n}{n+1 + \cfrac{n+1}{n+2 + \cfrac{n+2}{n+3 + \cfrac{n+3}{\ddots}}}} = -\frac{n}{n+1} \times \frac{x \sum_{k=0}^{n} \frac{(-1)^k}{k!} - 1}{x \sum_{k=0}^{n+1} \frac{(-1)^k}{k!} - 1}.$$

This subfraction formula provides a surprising twist for a proof by contradiction. Indeed, if $x \neq e$ then

$$\lim_{n \to \infty} u_n = -\frac{xe^{-1} - 1}{xe^{-1} - 1} = -1,$$

which is utterly untrue as $u_n > n$.

Similarly, for the second identity, suppose that the continued fraction converges to x, then, having proved:

$$v_n = n + \cfrac{n+1}{n+1+\cfrac{n+2}{n+2+\cfrac{n+3}{\ddots}}} = -\frac{x\sum_{k=0}^{n-1}\frac{(-1)^k}{k!} - 1}{x\sum_{k=0}^{n}\frac{(-1)^k}{k!} - 1},$$

if $x \neq e$ then

$$\lim_{n\to\infty} v_n = -\frac{xe^{-1}-1}{xe^{-1}-1} = -1,$$

which is utterly untrue as $v_n > n$, so $x = e$.

As a by-product, we obtain the following two new continued fractions

$$n + \cfrac{n}{n+1+\cfrac{n+1}{n+2+\cfrac{n+2}{n+3+\cfrac{n+3}{\ddots}}}} = -\frac{n}{n+1} \times \frac{e\sum_{k=0}^{n}\frac{(-1)^k}{k!} - 1}{e\sum_{k=0}^{n+1}\frac{(-1)^k}{k!} - 1},$$

and

$$n + \cfrac{n+1}{n+1+\cfrac{n+2}{n+2+\cfrac{n+3}{\ddots}}} = -\frac{e\sum_{k=0}^{n-1}\frac{(-1)^k}{k!} - 1}{e\sum_{k=0}^{n}\frac{(-1)^k}{k!} - 1}.$$

This chapter is based on the paper [43].

3.1 Proof of the first continued fraction result

Theorem 3.1.1 *For any integer $n \geq 1$,*

$$n + \cfrac{n}{n+1+\cfrac{n+1}{n+2+\cfrac{n+2}{n+3+\cfrac{n+3}{\ddots}}}} = -\frac{n}{n+1} \times \frac{e\sum_{k=0}^{n}\frac{(-1)^k}{k!} - 1}{e\sum_{k=0}^{n+1}\frac{(-1)^k}{k!} - 1},$$

and

$$2 + \cfrac{1}{1+\cfrac{1}{2+\cfrac{2}{3+\cfrac{3}{\ddots}}}} = e.$$

Proof. By Theorem 1.4.6, we know that the first continued fraction of (3.1) converges. Let x be this convergence value and construct the sequences $\{u_n\}$, $\{a_n\}$, $\{b_n\}$, $\{c_n\}$, $\{d_n\}$ as follows

$$u_1 = 1 + \cfrac{1}{2+\cfrac{2}{3+\cfrac{3}{\ddots}}} = \frac{1}{x-2} = \frac{xa_1 + b_1}{xc_1 + d_1},$$

$$
\begin{aligned}
u_n &= n + \cfrac{n}{n+1+\cfrac{n+1}{n+2+\cfrac{n+2}{\ddots}}} \\
&= \frac{n-1}{u_{n-1}-(n-1)} \\
&= \frac{n-1}{\dfrac{xa_{n-1}+b_{n-1}}{xc_{n-1}+d_{n-1}}-(n-1)} \\
&= \frac{x(n-1)c_{n-1}+(n-1)d_{n-1}}{x(a_{n-1}-(n-1)c_{n-1})+(b_{n-1}-(n-1)d_{n-1})} \\
&= \frac{xa_n+b_n}{xc_n+d_n}.
\end{aligned}
$$

Then we have the following recursive formulas

$$
\begin{aligned}
&a_1 = 0, \quad b_1 = 1, \quad c_1 = 1, \quad d_1 = -2, \\
&a_n = (n-1)c_{n-1}, \quad b_n = (n-1)d_{n-1}, \\
&c_n = a_{n-1} - (n-1)c_{n-1}, \quad d_n = b_{n-1} - (n-1)d_{n-1}, \quad \forall n \geq 2.
\end{aligned}
$$

For any $n \geq 3$, we have

$$
\begin{aligned}
& \frac{a_n}{n-1} = c_{n-1} = a_{n-2} - (n-2)c_{n-2} = a_{n-2} - a_{n-1} \\
\Rightarrow \quad & a_n + (n-1)a_{n-1} - (n-1)a_{n-2} = 0 \\
\Rightarrow \quad & a_n - a_{n-2} + (n-1)a_{n-1} - (n-2)a_{n-2} = 0.
\end{aligned}
$$

So

$$
\sum_{k=3}^{n} (a_k - a_{k-2} + (k-1)a_{k-1} - (k-2)a_{k-2}) = 0,
$$

which gives

$$
a_n + a_{n-1} - a_2 - a_1 + (n-1)a_{n-1} - a_1 = 0.
$$

It follows that for any $n \geq 2$,

$$
a_n + na_{n-1} = a_2 + 2a_1.
$$

Rewrite the above equation as

$$\frac{(-1)^n a_n}{n!} - \frac{(-1)^{n-1} a_{n-1}}{(n-1)!} = (a_2 + 2a_1)\frac{(-1)^n}{n!}$$

and taking the summation

$$\sum_{k=2}^{n} \left(\frac{(-1)^k a_k}{k!} - \frac{(-1)^{k-1} a_{k-1}}{(k-1)!} \right) = (a_2 + 2a_1) \sum_{k=2}^{n} \frac{(-1)^k}{k!}$$

we get

$$\frac{(-1)^n a_n}{n!} - \frac{(-1)a_1}{1!} = (a_2 + 2a_1) \sum_{k=2}^{n} \frac{(-1)^k}{k!}, \quad \forall n \geq 1.$$

We derive the following closed form for a_n:

$$a_n = (-1)^n n! \left(-a_1 + (a_2 + 2a_1) \sum_{k=0}^{n} \frac{(-1)^k}{k!} \right), \quad \forall n \geq 1.$$

Similarly, we get the following closed form for b_n:

$$b_n = (-1)^n n! \left(-b_1 + (b_2 + 2b_1) \sum_{k=0}^{n} \frac{(-1)^k}{k!} \right), \quad \forall n \geq 1.$$

Substituting the values

$$a_1 = 0, \quad b_1 = 1, \quad a_2 = 1, \quad b_2 = -2$$

we obtain

$$\begin{aligned} a_n &= (-1)^n n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \\ b_n &= (-1)^{n+1} n! \end{aligned}$$

It follows that

$$\begin{aligned} c_n &= \frac{a_{n+1}}{n} = (-1)^{n+1} \frac{(n+1)!}{n} \sum_{k=0}^{n+1} \frac{(-1)^k}{k!}, \\ d_n &= \frac{b_{n+1}}{n} = (-1)^n \frac{(n+1)!}{n}. \end{aligned}$$

Finally, we have

$$u_n = \frac{xa_n + b_n}{xc_n + d_n} = \frac{x(-1)^n n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} + (-1)^{n+1} n!}{x(-1)^{n+1} \frac{(n+1)!}{n} \sum_{k=0}^{n+1} \frac{(-1)^k}{k!} + (-1)^n \frac{(n+1)!}{n}}$$

$$= -\frac{n}{n+1} \frac{x \sum_{k=0}^{n} \frac{(-1)^k}{k!} - 1}{x \sum_{k=0}^{n+1} \frac{(-1)^k}{k!} - 1}, \quad \forall n \geq 1.$$

This implies that $x = e$ because if $x \neq e$ then

$$\lim_{n\to\infty} u_n = -\frac{xe^{-1} - 1}{xe^{-1} - 1} = -1$$

which contradicts the obvious fact that $u_n > n$. ■

3.2 Proof of the second continued fraction result

Theorem 3.2.1 *For any integer $n \geq 1$,*

$$n + \cfrac{n+1}{n+1 + \cfrac{n+2}{n+2 + \cfrac{n+3}{\ddots}}} = -\frac{e \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} - 1}{e \sum_{k=0}^{n} \frac{(-1)^k}{k!} - 1},$$

and

$$2 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{4 + \cfrac{5}{\ddots}}}} = e.$$

Proof. By Theorem 1.4.6, we know that the second continued fraction of (3.1) converges. Let x be this convergence value and construct the sequences $\{v_n\}$, $\{a_n\}$,

$\{b_n\}$, $\{c_n\}$, $\{d_n\}$ as follows

$$v_1 = 1 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{\ddots}}} = x - 1 = \frac{xa_1 + b_1}{xc_1 + d_1}$$

$$\begin{aligned} v_n &= n + \cfrac{n+1}{n+1 + \cfrac{n+2}{n+2 + \cfrac{n+3}{\ddots}}} \\ &= \frac{n}{v_{n-1} - (n-1)} \\ &= \frac{n}{\dfrac{xa_{n-1} + b_{n-1}}{xc_{n-1} + d_{n-1}} - (n-1)} \\ &= \frac{xnc_{n-1} + nd_{n-1}}{x(a_{n-1} - (n-1)c_{n-1}) + (b_{n-1} - (n-1)d_{n-1})} \\ &= \frac{xa_n + b_n}{xc_n + d_n}. \end{aligned}$$

Then we have the following recursive formulas

$$\begin{aligned} &a_1 = 1, \quad b_1 = -1, \quad c_1 = 0, \quad d_1 = 1, \\ &a_n = nc_{n-1}, \quad b_n = nd_{n-1}, \\ &c_n = a_{n-1} - (n-1)c_{n-1}, \quad d_n = b_{n-1} - (n-1)d_{n-1}, \quad \forall n \geq 2. \end{aligned}$$

For any $n \geq 3$,

$$\begin{aligned} & c_n = a_{n-1} - (n-1)c_{n-1} = (n-1)c_{n-2} - (n-1)c_{n-1} \\ \Rightarrow \quad & c_n + (n-1)c_{n-1} - (n-1)c_{n-2} = 0 \\ \Rightarrow \quad & c_n - c_{n-1} + nc_{n-1} - (n-1)c_{n-2} = 0. \end{aligned}$$

Taking summation

$$\sum_{k=3}^{n} (c_k - c_{k-1} + kc_{k-1} - (k-1)c_{k-2}) = 0$$

and we get

$$c_n - c_2 + nc_{n-1} - 2c_1 = 0.$$

We have

$$c_n + nc_{n-1} = c_2 + 2c_1, \quad \forall n \geq 2$$

so

$$\frac{(-1)^n c_n}{n!} - \frac{(-1)^{n-1} c_{n-1}}{(n-1)!} = (c_2 + 2c_1)\frac{(-1)^n}{n!}.$$

Taking summation again

$$\sum_{k=2}^{n} \left(\frac{(-1)^k c_k}{k!} - \frac{(-1)^{k-1} c_{k-1}}{(k-1)!} \right) = (c_2 + 2c_1) \sum_{k=2}^{n} \frac{(-1)^k}{k!}$$

and we get

$$\frac{(-1)^n c_n}{n!} - \frac{(-1)c_1}{1!} = (c_2 + 2c_1) \sum_{k=2}^{n} \frac{(-1)^k}{k!}, \quad \forall n \geq 1.$$

Therefore,

$$c_n = (-1)^n n! \left(-c_1 + (c_2 + 2c_1) \sum_{k=0}^{n} \frac{(-1)^k}{k!} \right), \quad \forall n \geq 1$$

and similarly,

$$d_n = (-1)^n n! \left(-d_1 + (d_2 + 2d_1) \sum_{k=0}^{n} \frac{(-1)^k}{k!} \right), \quad \forall n \geq 1$$

Substituting the values

$$c_1 = 0, \quad d_1 = 1, \quad c_2 = 1, \quad d_2 = -2,$$

we obtain

$$c_n = (-1)^n n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$
$$d_n = (-1)^{n+1} n!$$

It follows that

$$a_n = nc_{n-1} = (-1)^{n-1} n! \sum_{k=0}^{n-1} \frac{(-1)^k}{k!}$$
$$b_n = nd_{n-1} = (-1)^n n!$$

Finally,

$$v_n = \frac{xa_n + b_n}{xc_n + d_n} = \frac{x(-1)^{n-1}n! \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} + (-1)^n n!}{x(-1)^n n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} + (-1)^{n+1} n!}$$

$$= -\frac{x \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} - 1}{x \sum_{k=0}^{n} \frac{(-1)^k}{k!} - 1}, \quad \forall n \geq 1.$$

So, if $x \neq e$ we would have $\lim_{n\to\infty} v_n = -1$, which contradicts the fact that $v_n > n$. Therefore, $x = e$. ■

Chapter 4

A "New Year" Continued Fraction

In the *Mathematics Magazine*, December 2014 issue [40], the following continued fraction is displayed to celebrate the new year

$$2014 = 2015 - \cfrac{1 \times 2015}{2017 - \cfrac{2 \times 2016}{2019 - \cfrac{3 \times 2017}{2021 - \cfrac{4 \times 2018}{\ddots}}}}$$

In this chapter, we will prove a general form of this continued fraction

$$a + 1 - \cfrac{1(a+1)}{a + 3 - \cfrac{2(a+2)}{a + 5 - \cfrac{3(a+3)}{a + 7 - \cfrac{4(a+4)}{\ddots}}}} = \begin{cases} a & \text{if } a \geq 0 \\ \\ 0 & \text{if } a < 0 \text{ and } a \notin \mathbb{Z} \end{cases} \tag{4.1}$$

We derive the previous infinite continued fraction from the following finite continued fraction

$$a+1-\cfrac{1(a+1)}{a+3-\cfrac{2(a+2)}{a+5-\cfrac{3(a+3)}{\ddots\quad a+2n-1-\cfrac{n(a+n)}{a+2n+1}}}}$$

$$=\begin{cases}\cfrac{1}{\sum_{k=0}^{n}\cfrac{1}{k+1}} & \text{if } a=0\\[2ex] \cfrac{a}{1-\cfrac{(n+1)!}{(a+1)(a+2)\dots(a+n+1)}} & \text{if } a\neq 0\end{cases}$$

The following identity due to Euler is a useful identity for generating continued fractions

$$\cfrac{1}{\cfrac{1}{\alpha_1}-\cfrac{1}{\alpha_2}+\cfrac{1}{\alpha_3}-\cfrac{1}{\alpha_4}+\dots}=\alpha_1+\cfrac{\alpha_1^2}{\alpha_2-\alpha_1+\cfrac{\alpha_2^2}{\alpha_3-\alpha_2+\cfrac{\alpha_3^2}{\alpha_4-\alpha_3+\cfrac{\alpha_4^2}{\ddots}}}}. \tag{4.2}$$

If we take $\alpha_k=(-1)^{k+1}k$ and equate $1/\left(\sum_{k=1}^{\infty}\frac{1}{k}\right)$ to 0, we obtain the following interesting continued fraction for zero

$$0=1-\cfrac{1^2}{3-\cfrac{2^2}{5-\cfrac{3^2}{7-\cfrac{4^2}{\ddots}}}} \tag{4.3}$$

Inductively, we can derive from (4.3) the following

$$1 = 3 - \cfrac{2^2}{5 - \cfrac{3^2}{7 - \cfrac{4^2}{9 - \cfrac{5^2}{\ddots}}}},$$

$$2 = 5 - \cfrac{3^2}{7 - \cfrac{4^2}{9 - \cfrac{5^2}{11 - \cfrac{6^2}{\ddots}}}},$$

and in general

$$a = 2a + 1 - \cfrac{(a+1)^2}{2a + 3 - \cfrac{(a+2)^2}{2a + 5 - \cfrac{(a+3)^2}{2a + 7 - \cfrac{(a+4)^2}{\ddots}}}}.$$

We can see that the identity (4.3) is a special case of our identity (4.1) when $a = 0$. However, while the identity (4.3) is obtained from Euler's identity (4.2), our identity (4.1) is not. Moreover, our identity (4.1) holds for all *positive real* numbers a.

This chapter is based on the paper [42].

4.1 The finite continued fraction

In order to prove (4.1), we will establish a closed form formula for its convergents – which is the following finite continued fraction.

Theorem 4.1.1 *For any natural number n, and for any complex number a which*

is not a negative integer, we have

$$a+1-\cfrac{1(a+1)}{a+3-\cfrac{2(a+2)}{a+5-\cfrac{3(a+3)}{\ddots\quad a+2n-1-\cfrac{n(a+n)}{a+2n+1}}}}$$

$$=\begin{cases}\dfrac{1}{\sum_{k=0}^{n}\dfrac{1}{k+1}} & \text{if } a=0\\[2ex] \dfrac{a}{1-\dfrac{(n+1)!}{(a+1)(a+2)\dots(a+n+1)}} & \text{if } a\neq 0\end{cases}$$

Proof. By the Euler-Wallis formulas,

$$\begin{aligned} &p_{-2}=0,\quad p_{-1}=1,\quad p_n=(a+2n+1)p_{n-1}-n(a+n)p_{n-2}\quad \forall n\geq 0\\ &q_{-1}=0,\quad q_0=1,\quad q_n=(a+2n+1)q_{n-1}-n(a+n)q_{n-2}\quad \forall n\geq 1\end{aligned}$$

We rewrite the recurrence formula as

$$q_n-nq_{n-1}=(a+n+1)q_{n-1}-n(a+n)q_{n-2}$$

and

$$\frac{q_n}{n!}-\frac{q_{n-1}}{(n-1)!}=\frac{(a+n+1)q_{n-1}}{n!}-\frac{(a+n)q_{n-2}}{(n-1)!}.$$

Taking the summation we obtain

$$\frac{q_n}{n!}-q_0=\frac{(a+n+1)q_{n-1}}{n!}-(a+1)q_{-1}$$

so

$$q_n-(a+n+1)q_{n-1}=(q_0-(a+1)q_{-1})n!\ .$$

Using the Gamma function [16], which is defined for all complex numbers except the non-positive integers, with the identity $\Gamma(z+1)=z\Gamma(z)$, rewrite the above equation as

$$\frac{q_n}{\Gamma(a+n+2)}-\frac{q_{n-1}}{\Gamma(a+n+1)}=(q_0-(a+1)q_{-1})\frac{n!}{\Gamma(n+a+2)}$$

and taking the summation again we get

$$\frac{q_n}{\Gamma(a+n+2)} - \frac{q_{-1}}{\Gamma(a+1)} = (q_0 - (a+1)q_{-1}) \sum_{k=0}^{n} \frac{k!}{\Gamma(k+a+2)}$$

so

$$\frac{q_n}{\Gamma(a+n+2)} = \frac{q_{-1}}{\Gamma(a+1)} + (q_0 - (a+1)q_{-1}) \sum_{k=0}^{n} \frac{k!}{\Gamma(k+a+2)}$$

Similarly, we have

$$\frac{p_n}{\Gamma(a+n+2)} = \frac{p_{-1}}{\Gamma(a+1)} + (p_0 - (a+1)p_{-1}) \sum_{k=0}^{n} \frac{k!}{\Gamma(k+a+2)}$$

Substitute the values $q_{-1} = 0$, $q_0 = 1$, $p_{-1} = 1$, $p_0 = a+1$, we obtain

$$\begin{aligned} \frac{q_n}{\Gamma(a+n+2)} &= \sum_{k=0}^{n} \frac{k!}{\Gamma(k+a+2)} \\ \frac{p_n}{\Gamma(a+n+2)} &= \frac{1}{\Gamma(a+1)} \end{aligned}$$

Thus, we have the following closed form formula for the convergent

$$\frac{p_n}{q_n} = \frac{1}{\Gamma(a+1) \sum_{k=0}^{n} \frac{k!}{\Gamma(k+a+2)}}$$

There are two cases.

Case 1: if $a = 0$ then

$$\frac{p_n}{q_n} = \frac{1}{\sum_{k=0}^{n} \frac{1}{k+1}}$$

Case 2: if $a \neq 0$, we use the following identity

$$\frac{k!}{\Gamma(k+a+1)} - \frac{(k+1)!}{\Gamma(k+a+2)} = \frac{k!}{\Gamma(k+a+2)} \left((k+a+1) - (k+1)\right) = a \frac{k!}{\Gamma(k+a+2)},$$

then

$$\begin{aligned}\frac{p_n}{q_n} &= \frac{1}{\Gamma(a)\sum_{k=0}^{n}\left(\dfrac{k!}{\Gamma(k+a+1)}-\dfrac{(k+1)!}{\Gamma(k+a+2)}\right)} \\ &= \frac{1}{\Gamma(a)\left(\dfrac{1}{\Gamma(a+1)}-\dfrac{(n+1)!}{\Gamma(n+a+2)}\right)}\end{aligned} \tag{4.4}$$

and finally,

$$\frac{p_n}{q_n} = \frac{a}{1-\dfrac{(n+1)!}{(a+1)(a+2)\dots(a+n+1)}} \tag{4.5}$$

This completes the proof. ■

4.2 The infinite continued fraction

Having established the closed form formula for the convergent in Theorem 4.1.1, we are now ready to derive the main continued fraction in Theorem 4.2.1.

Theorem 4.2.1 *For any real number a,*

$$a+1-\cfrac{1(a+1)}{a+3-\cfrac{2(a+2)}{a+5-\cfrac{3(a+3)}{a+7-\cfrac{4(a+4)}{\ddots}}}} = \begin{cases} a & \text{if } a \geq 0 \\ 0 & \text{if } a < 0 \text{ and } a \notin \mathbb{Z} \end{cases} \tag{4.6}$$

Proof. The case $a = 0$ is the identity (4.3). When $a > 0$, we have

$$\begin{aligned}\frac{(a+1)(a+2)\dots(a+n+1)}{(n+1)!} &= (1+\frac{a}{1})(1+\frac{a}{2})\dots(1+\frac{a}{n})(1+\frac{a}{n+1}) \\ &> 1+\frac{a}{1}+\frac{a}{2}+\dots+\frac{a}{n}+\frac{a}{n+1} \to +\infty\end{aligned}$$

So from (4.5), we have $\lim_{n\to\infty}\frac{p_n}{q_n} = a$ and the theorem follows.

When $a < -1$ and $a \notin \mathbb{Z}$, let $A = \lfloor -a \rfloor \geq 1$, then $0 < a + A + 1 < 1$ and we have

$$0 < \frac{(a+A+1)(a+A+2)\dots(a+n+1)}{1 \times 2 \times \cdots \times (n+1-A)} < 1$$

so

$$0 < \frac{(a+A+1)(a+A+2)\dots(a+n+1)}{(n+1)!} < \frac{1}{n+1} \to 0.$$

Hence, from (4.5), we have $\lim_{n\to\infty} \frac{p_n}{q_n} = 0$ and the theorem follows.

When $-1 < a < 0$, using the following well-known limit [1] that, for any complex number α,

$$\lim_{n\to\infty} \frac{\Gamma(n+\alpha)}{\Gamma(n)\, n^{\alpha}} = 1,$$

we have

$$\lim_{n\to\infty} \frac{\Gamma(n+a+2)}{(n+1)!} = \lim_{n\to\infty} \frac{\Gamma(n+a+2)}{\Gamma(n)\, n^{a+2}} \frac{n^{a+1}}{n+1} = 1 \times 0 = 0.$$

So from (4.4), we have $\lim_{n\to\infty} \frac{p_n}{q_n} = 0$ and the theorem follows. ■

Chapter 5

The First Two Harmonic Continued Fractions

Define *harmonic continued fractions* [12] by:

$$HCF(t) = \frac{t}{1} + \cfrac{1}{\frac{t}{2} + \cfrac{1}{\frac{t}{3} + \cfrac{1}{\ddots}}}.$$

Since the harmonic series $\sum \frac{1}{n}$ diverges, by the Seidel-Stern Theorem (Theorem 1.4.8), the continued fraction $HCF(t)$ converges for any positive real number t.

In this chapter, we study $HCF(1)$ and $HCF(2)$ and show that

$$HCF(1) = \frac{1}{1} + \cfrac{1}{\frac{1}{2} + \cfrac{1}{\frac{1}{3} + \cfrac{1}{\frac{1}{4} + \cfrac{1}{\ddots}}}} = \frac{2}{\pi - 2}$$

and

$$HCF(2) = \frac{2}{1} + \cfrac{1}{\frac{2}{2} + \cfrac{1}{\frac{2}{3} + \cfrac{1}{\frac{2}{4} + \cfrac{1}{\ddots}}}} = \frac{1}{2\ln 2 - 1}.$$

The values of $HCF(1)$ and $HCF(2)$ can be derived from the following continued fractions of Euler [20]:

$$1+\cfrac{1}{1+\cfrac{1\times 2}{1+\cfrac{2\times 3}{1+\cfrac{3\times 4}{1+\ddots}}}}=\frac{\pi}{2},\qquad 2+\cfrac{1\times 2}{2+\cfrac{2\times 3}{2+\cfrac{3\times 4}{2+\cfrac{4\times 5}{2+\ddots}}}}=\frac{1}{2\ln 2-1}.$$

Euler's proof involved the Wallis product and differential equations. Another elementary proof for $HCF(1)$ was given by Pickett and Coleman [36] in 2008. In this chapter, we offer an elementary and direct proof. Our proof uses the Euler-Wallis recurrence formula to establish the following *closed form formulas* for the convergents of the continued fractions $HCF(1)$ and $HCF(2)$:

$$\frac{1}{1}+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{1}{2n-1}}}}}=\cfrac{1}{\frac{1}{2n}\,\frac{2^2 4^2\ldots(2n)^2}{1^2 3^2\ldots(2n-1)^2}-1},$$

$$\frac{1}{1}+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{1}{2n}}}}}=\cfrac{1}{\frac{1}{2n+1}\,\frac{2^2 4^2\ldots(2n)^2}{1^2 3^2\ldots(2n-1)^2}-1},$$

$$\frac{2}{1}+\cfrac{1}{\frac{2}{2}+\cfrac{1}{\frac{2}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{2}{n}}}}}=\cfrac{1}{\sum\limits_{i=0}^{n-1}\frac{(-1)^i}{(i+1)(i+2)}}.$$

This chapter is based on the paper [12].

5.1 HCF(1)

The following theorem establishes closed form formulas for the numerator p_n and the denominator q_n of the convergents of $HCF(1)$.

Theorem 5.1.1 *The numerator p_n and the denominator q_n of the convergents of $HCF(1)$ are*

$$\begin{aligned}
p_{2n} &= \prod_{i=1}^{n} \frac{2i+1}{2i}, \quad \forall n \geq 0, \\
p_{2n+1} &= \prod_{i=1}^{n+1} \frac{2i+1}{2i}, \quad \forall n \geq 0, \\
q_{2n} &= \left(\frac{1}{2n+2} \frac{2^2 4^2 \dots (2n+2)^2}{1^2 3^2 \dots (2n+1)^2} - 1 \right) \prod_{i=1}^{n} \frac{2i+1}{2i}, \quad \forall n \geq 0, \\
q_{2n+1} &= \left(\frac{1}{2n+3} \frac{2^2 4^2 \dots (2n+2)^2}{1^2 3^2 \dots (2n+1)^2} - 1 \right) \prod_{i=1}^{n+1} \frac{2i+1}{2i}, \quad \forall n \geq 0.
\end{aligned}$$

Proof. By Theorem 1.4.2,

$$\begin{aligned}
p_n &= \left(\frac{1}{n(n+1)} + \frac{n-1}{n+1} + 1 \right) p_{n-2} - \frac{n-1}{n+1} p_{n-4} \\
&= \frac{2n^2+1}{n(n+1)} p_{n-2} - \frac{n-1}{n+1} p_{n-4}, \quad \forall n \geq 2
\end{aligned}$$

So

$$\begin{aligned}
p_{2n} &= \frac{8n^2+1}{2n(2n+1)} p_{2n-2} - \frac{2n-1}{2n+1} p_{2n-4}, \quad \forall n \geq 1, \\
p_{2n+1} &= \frac{8n^2+8n+3}{(2n+1)(2n+2)} p_{2n-1} - \frac{2n}{2n+2} p_{2n-3}, \quad \forall n \geq 1.
\end{aligned}$$

For each $n \geq -1$, let

$$p_{2n} = p'_{2n} \prod_{i=1}^{n} \frac{2i+1}{2i} \quad \text{and} \quad p_{2n+1} = p'_{2n+1} \prod_{i=1}^{n+1} \frac{2i+1}{2i},$$

then

$$\frac{2n+1}{2n}\frac{2n-1}{2n-2}\,p'_{2n} = \frac{8n^2+1}{2n(2n+1)}\frac{2n-1}{2n-2}\,p'_{2n-2} - \frac{2n-1}{2n+1}\,p'_{2n-4}, \quad \forall n \geq 2,$$
$$\frac{2n+3}{2n+2}\frac{2n+1}{2n}\,p'_{2n+1} = \frac{8n^2+8n+3}{(2n+1)(2n+2)}\frac{2n+1}{2n}\,p'_{2n-1} - \frac{2n}{2n+2}\,p'_{2n-3}, \quad \forall n \geq 1.$$

This simplifies to

$$(2n+1)^2\,p'_{2n} = (8n^2+1)\,p'_{2n-2} - 2n(2n-2)\,p'_{2n-4}, \quad \forall n \geq 2,$$
$$(2n+3)(2n+1)\,p'_{2n+1} = (8n^2+8n+3)\,p'_{2n-1} - 4n^2\,p'_{2n-3}, \quad \forall n \geq 1,$$

and so,

$$(2n+1)^2\,(p'_{2n} - p'_{2n-2}) = 2n(2n-2)\,(p'_{2n-2} - p'_{2n-4}), \quad \forall n \geq 2$$
$$(2n+3)(2n+1)\,(p'_{2n+1} - p'_{2n-1}) = 4n^2\,(p'_{2n-1} - p'_{2n-3}), \quad \forall n \geq 1$$

Therefore,

$$p'_{2n} - p'_{2n-2} = \frac{2n(2n-2)}{(2n+1)^2}\,(p'_{2n-2} - p'_{2n-4}), \quad \forall n \geq 2, \tag{5.1}$$
$$p'_{2n+1} - p'_{2n-1} = \frac{4n^2}{(2n+3)(2n+1)}\,(p'_{2n-1} - p'_{2n-3}), \quad \forall n \geq 1. \tag{5.2}$$

We have $p_{-1} = 1$, $p_0 = 1$, $p_1 = \frac{3}{2}$, $p_2 = \frac{3}{2}$, so

$$p'_{-1} = p'_0 = p'_1 = p'_2 = 1.$$

It follows that

$$p'_n = 1, \quad \forall n \geq -1.$$

This gives us the desired closed form formula for p_n:

$$p_{2n} = \prod_{i=1}^{n} \frac{2i+1}{2i} \quad \text{and} \quad p_{2n+1} = \prod_{i=1}^{n+1} \frac{2i+1}{2i}, \quad \forall n \geq 0.$$

Defining a sequence $\{q'_n\}$ for $\{q_n\}$ similar to $\{p'_n\}$ for $\{p_n\}$, we seek for $\{q'_n\}$ equations corresponding to (5.1) and (5.2). With $q_{-1} = 0$, $q_0 = 1$, $q_1 = \frac{1}{2}$, $q_2 = \frac{7}{6}$, we have

$$q'_{-1} = 0, \quad q'_0 = 1, \quad q'_1 = \frac{1}{3}, \quad q'_2 = \frac{7}{9}.$$

This gives us

$$\begin{aligned}
q'_{2n} - q'_{2n-2} &= \frac{2n(2n-2)}{(2n+1)^2} \cdots \frac{(4)(2)}{5^2}(q'_2 - q'_0) \\
&= -\frac{2n(2n-2)}{(2n+1)^2} \cdots \frac{(4)(2)}{5^2}\frac{2}{9} \\
&= -\frac{1}{2n}\frac{2^2 4^2 \ldots (2n)^2}{1^2 3^2 \ldots (2n+1)^2}, \quad \forall n \geq 1, \\
q'_{2n+1} - q'_{2n-1} &= \frac{(2n)^2}{(2n+3)(2n+1)} \cdots \frac{2^2}{(5)(3)}(q'_1 - q'_{-1}) \\
&= \frac{(2n)^2}{(2n+3)(2n+1)} \cdots \frac{2^2}{(5)(3)}\frac{1}{3} \\
&= \frac{1}{2n+3}\frac{2^2 4^2 \ldots (2n)^2}{1^2 3^2 \ldots (2n+1)^2}, \quad \forall n \geq 1.
\end{aligned}$$

Simple algebraic manipulation gives us

$$\begin{aligned}
q'_{2n} - q'_{2n-2} &= \frac{1}{2n+2}\frac{2^2 4^2 \ldots (2n+2)^2}{1^2 3^2 \ldots (2n+1)^2} - \frac{1}{2n}\frac{2^2 4^2 \ldots (2n)^2}{1^2 3^2 \ldots (2n-1)^2}, \quad \forall n \geq 1, \\
q'_{2n+1} - q'_{2n-1} &= \frac{1}{2n+3}\frac{2^2 4^2 \ldots (2n+2)^2}{1^2 3^2 \ldots (2n+1)^2} - \frac{1}{2n+1}\frac{2^2 4^2 \ldots (2n)^2}{1^2 3^2 \ldots (2n-1)^2}, \quad \forall n \geq 1.
\end{aligned}$$

Replacing n by i and summing over i, from 1 to n, we find that

$$\begin{aligned}
q'_{2n} - q'_0 &= \frac{1}{2n+2}\frac{2^2 4^2 \ldots (2n+2)^2}{1^2 3^2 \ldots (2n+1)^2} - \frac{1}{2}\frac{2^2}{1^2}, \quad \forall n \geq 0, \\
q'_{2n+1} - q'_1 &= \frac{1}{2n+3}\frac{2^2 4^2 \ldots (2n+2)^2}{1^2 3^2 \ldots (2n+1)^2} - \frac{1}{3}\frac{2^2}{1^2}, \quad \forall n \geq 0.
\end{aligned}$$

Therefore,

$$\begin{aligned}
q'_{2n} &= \frac{1}{2n+2}\frac{2^2 4^2 \ldots (2n+2)^2}{1^2 3^2 \ldots (2n+1)^2} - 1, \quad \forall n \geq 0, \\
q'_{2n+1} &= \frac{1}{2n+3}\frac{2^2 4^2 \ldots (2n+2)^2}{1^2 3^2 \ldots (2n+1)^2} - 1, \quad \forall n \geq 0.
\end{aligned}$$

From here we obtain the desired closed form formula for q_n. ■

The following theorem is a consequence of Theorem 5.1.1.

Theorem 5.1.2 *For any natural number $n \geq 1$,*

$$\frac{1}{1}+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{1}{2n-1}}}}} = \frac{1}{\frac{1}{2n}\,\frac{2^2 4^2 \dots (2n)^2}{1^2 3^2 \dots (2n-1)^2}-1},$$

$$\frac{1}{1}+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{1}{2n}}}}} = \frac{1}{\frac{1}{2n+1}\,\frac{2^2 4^2 \dots (2n)^2}{1^2 3^2 \dots (2n-1)^2}-1}.$$

We are now ready to determine the value of $HCF(1)$.

Theorem 5.1.3

$$HCF(1) = \frac{1}{1}+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\frac{1}{4}+\cfrac{1}{\ddots}}}} = \frac{2}{\pi-2}$$

Proof. By Theorem 5.1.1,

$$\frac{q_{2n}}{p_{2n}} = \frac{1}{2n+2}\frac{2^2 4^2 \dots (2n+2)^2}{1^2 3^2 \dots (2n+1)^2}-1,$$
$$\frac{q_{2n+1}}{p_{2n+1}} = \frac{1}{2n+3}\frac{2^2 4^2 \dots (2n+2)^2}{1^2 3^2 \dots (2n+1)^2}-1.$$

We have,

$$\begin{aligned}\Gamma\left(n+\frac{3}{2}\right) &= \left(n+\frac{1}{2}\right)\Gamma\left(n+\frac{1}{2}\right) = \left(n+\frac{1}{2}\right)\left(n-\frac{1}{2}\right)\Gamma\left(n-\frac{1}{2}\right) \\ &= \left(n+\frac{1}{2}\right)\left(n-\frac{1}{2}\right)\cdots\frac{1}{2}\Gamma\left(\frac{1}{2}\right) \\ &= \frac{2n+1}{2}\frac{2n-1}{2}\cdots\frac{1}{2}\sqrt{\pi}.\end{aligned}$$

It follows that

$$\frac{q_{2n}}{p_{2n}} = \frac{\pi}{2}\frac{(n+1)\Gamma(n+1)^2}{\Gamma(n+\frac{3}{2})^2} - 1 \to \frac{\pi}{2} - 1.$$

The above limit is due to the fact [1] that, for any complex number a,

$$\lim_{n\to\infty}\frac{n^a\ \Gamma(n)}{\Gamma(n+a)} = 1,$$

we have used $a = \frac{1}{2}$.

Further

$$\lim_{n\to\infty}\frac{q_{2n+1}}{p_{2n+1}} = \lim_{n\to\infty}\frac{q_{2n}}{p_{2n}} = \frac{\pi}{2} - 1.$$

The reciprocal of this limit shows that $HCF(1) = \frac{2}{\pi-2} \approx 1.75$. ■

5.2 HCF(2)

The following theorem establishes closed form formulas for the numerator p_n and the denominator q_n of the convergents of $HCF(2)$.

Theorem 5.2.1 *For any $n \geq 0$, the numerator p_n and the denominator q_n of the convergents of $HCF(2)$ are*

$$\begin{aligned}p_n &= n+2, \\ q_n &= (n+2)\sum_{i=0}^{n}\frac{(-1)^i}{(i+1)(i+2)}.\end{aligned}$$

Proof. By the Euler-Wallis formula, the convergents $\frac{p_n}{q_n}$ are determined by the following recurrence relations

$$\begin{aligned} p_{-2} = 0,\ p_{-1} = 1,\ p_n &= \frac{2}{n+1}\ p_{n-1} + p_{n-2}, \quad \forall n \geq 0, \\ q_{-2} = 1,\ q_{-1} = 0,\ q_n &= \frac{2}{n+1}\ q_{n-1} + q_{n-2}, \quad \forall n \geq 0. \end{aligned}$$

We have

$$\begin{aligned} (n+1)p_n &= 2p_{n-1} + (n+1)p_{n-2}, \quad \forall n \geq 0, \\ (n+1)p_n + np_{n-1} &= (n+2)p_{n-1} + (n+1)p_{n-2}, \quad \forall n \geq 0, \\ (-1)^n(n+1)p_n - (-1)^{n-1}np_{n-1} &= (-1)^n(n+2)p_{n-1} - (-1)^{n-1}(n+1)p_{n-2}, \quad \forall n \geq 0. \end{aligned}$$

Taking summation, we have

$$\begin{aligned} (-1)^n(n+1)p_n &= (-1)^n(n+2)p_{n-1} - (-1)^{-1}p_{-2}, \quad \forall n \geq 0, \\ (n+1)p_n &= (n+2)p_{n-1} + (-1)^n p_{-2}, \quad \forall n \geq 0. \end{aligned}$$

Since $p_{-2} = 0$, it follows that

$$\begin{aligned} (n+1)p_n &= (n+2)p_{n-1}, \quad \forall n \geq 0, \\ \frac{p_n}{n+2} &= \frac{p_{n-1}}{n+1} = \cdots = \frac{p_{-1}}{1} = 1, \quad \forall n \geq 0, \\ p_n &= n+2, \quad \forall n \geq 0. \end{aligned}$$

Similarly,

$$(n+1)q_n = (n+2)q_{n-1} + (-1)^n q_{-2}, \quad \forall n \geq 0.$$

Since $q_{-2} = 1$, it follows that

$$\begin{aligned} (n+1)q_n &= (n+2)q_{n-1} + (-1)^n, \quad \forall n \geq 0, \\ \frac{q_n}{n+2} &= \frac{q_{n-1}}{n+1} + \frac{(-1)^n}{(n+1)(n+2)}, \quad \forall n \geq 0. \end{aligned}$$

Replacing n by i and summing from $i = 0$ to $i = n$, we obtain

$$\frac{q_n}{n+2} = \frac{q_{-1}}{1} + \sum_{i=0}^{n} \frac{(-1)^i}{(i+1)(i+2)} = \sum_{i=0}^{n} \frac{(-1)^i}{(i+1)(i+2)}, \quad \forall n \geq 0,$$

and this gives the desired closed form formula for q_n. ■

The following theorem is a consequence of Theorem 5.2.1.

Theorem 5.2.2 *For any natural number $n \geq 1$,*

$$\frac{2}{1}+\cfrac{1}{\frac{2}{2}+\cfrac{1}{\frac{2}{3}+\cfrac{1}{\ddots+\cfrac{1}{\frac{2}{n}}}}} = \frac{1}{\sum_{i=0}^{n-1}\frac{(-1)^i}{(i+1)(i+2)}}.$$

We are now ready to determine the value of $HCF(2)$.

Theorem 5.2.3

$$HCF(2) = \frac{2}{1}+\cfrac{1}{\frac{2}{2}+\cfrac{1}{\frac{2}{3}+\cfrac{1}{\frac{2}{4}+\cfrac{1}{\ddots}}}} = \frac{1}{2\ln 2-1}$$

Proof. By Theorem 5.2.1,

$$\frac{q_n}{p_n} = \sum_{i=0}^{n}\frac{(-1)^i}{(i+1)(i+2)}$$

So

$$\begin{aligned}\lim_{n\to\infty}\frac{q_n}{p_n} &= \lim_{n\to\infty}\sum_{i=0}^{n}\frac{(-1)^i}{(i+1)(i+2)} = \lim_{n\to\infty}\sum_{i=0}^{n}(-1)^i\left(\frac{1}{i+1}-\frac{1}{i+2}\right)\\ &= \lim_{n\to\infty}\sum_{i=0}^{n}\left(\frac{(-1)^i}{i+1}+\frac{(-1)^{i+1}}{i+2}\right)\\ &= -1+2\lim_{n\to\infty}\sum_{i=0}^{n}\frac{(-1)^i}{i+1} = 2\ln 2-1.\end{aligned}$$

The reciprocal of this limit gives $HCF(2) = \frac{1}{2\ln 2-1} \approx 2.59$. ■

Chapter 6

The General Harmonic Continued Fractions

In this chapter, we consider the *harmonic continued fraction*

$$HCF(t) = \frac{t}{1} + \cfrac{1}{\frac{t}{2} + \cfrac{1}{\frac{t}{3} + \cfrac{1}{\ddots}}},$$

for a general value of $t \in \mathbb{R}^+$.

Since the harmonic series $\sum \frac{1}{n}$ diverges, by the Seidel-Stern Theorem (Theorem 1.4.8), the continued fraction $HCF(t)$ converges for any positive real number t.

In Chapter 5, we studied $HCF(1)$ and $HCF(2)$ and showed that

$$HCF(1) = \frac{1}{1} + \cfrac{1}{\frac{1}{2} + \cfrac{1}{\frac{1}{3} + \cfrac{1}{\frac{1}{4} + \cfrac{1}{\ddots}}}} = \frac{2}{\pi - 2}$$

and

$$HCF(2) = \frac{2}{1} + \cfrac{1}{\frac{2}{2} + \cfrac{1}{\frac{2}{3} + \cfrac{1}{\frac{2}{4} + \cfrac{1}{\ddots}}}} = \frac{1}{2\ln 2 - 1}.$$

In this chapter, we study $HCF(t)$ for $t \in \mathbb{R}^+$ and derive explicit formulas for the numerator and the denominator of the convergents. In particular, when $t = 2a$ is an even positive integer, we can determine the exact value of $HCF(t)$ (Theorem 6.6.1):

$$HCF(2a) = \frac{(-1)^{a-1}}{2a\,\ln 2 - 1 - 2a\left(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{2\lfloor \frac{a}{2} \rfloor}\right)}.$$

Here are the first five harmonic continued fractions for the even case:

$$\begin{aligned}
HCF(2) &= \frac{1}{2\ln 2 - 1} \approx 2.59,\\
HCF(4) &= \frac{1}{3 - 4\ln 2} \approx 4.40,\\
HCF(6) &= \frac{1}{6\ln 2 - 4} \approx 6.29,\\
HCF(8) &= \frac{1}{\frac{17}{3} - 8\ln 2} \approx 8.23,\\
HCF(10) &= \frac{1}{10\ln 2 - \frac{41}{6}} \approx 10.19.
\end{aligned}$$

In order to establish this result, we define and study the following *convolution alternating power sums*

$$T_{i,j}(n) = \sum_{k=0}^{n} (-1)^k k^i (n-k)^j$$

and prove some identities involving Euler polynomials and Stirling numbers, which are of independent interest.

What about the case where t is an odd integer? As in all the cases where t is even, the value of $HCF(t)$ is written in terms of $\ln 2$, and $HCF(1) = \frac{2}{\pi - 2}$, we conjecture that for t is an odd integer, $HCF(t)$ is a simple rational function of π. It is our future work to determine this function.

6.1 Some preliminary results

We will use $f^{(n)}$ to denote the n^{th} derivative of a function f.

We will use $x_{[n]}$ and $x^{[n]}$ to denote the falling and rising factorials; $\begin{bmatrix} n \\ k \end{bmatrix}$ and $s_1(n,k)$ the unsigned and signed Stirling numbers of the first kind; and $s_2(n,k)$ the Stirling numbers of the second kind [1], which can be defined as

$$x_{[n]} = x(x-1)(x-2)\dots(x-n+1) = \sum_{k=0}^{n} s_1(n,k)x^k, \tag{6.1}$$

$$x^{[n]} = x(x+1)\dots(x+n-1) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k, \tag{6.2}$$

$$x^n = \sum_{k=0}^{n} s_2(n,k)x_{[k]}. \tag{6.3}$$

We have

$$s_1(n,k) = (-1)^{n+k} \begin{bmatrix} n \\ k \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} n \\ k \end{bmatrix} = |s_1(n,k)|. \tag{6.4}$$

Throughout this paper, $E_n(x)$ denotes an Euler polynomial. Euler polynomials can be defined using the generating series

$$\frac{2e^{xz}}{e^z+1} = \sum_{i=0}^{\infty} E_i(x)\frac{z^i}{i!}, \tag{6.5}$$

Here are the first few Euler polynomials: $E_0(x) = 1$, $E_1(x) = x - \frac{1}{2}$, $E_2(x) = x^2 - x$, $E_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{4}$, $E_4(x) = x^4 - 2x^3 + x$. The following are some well-known properties of the Euler polynomials [1], [14]:

$$E_n(-x) = (-1)^n\ (2x^n - E_n(x)), \tag{6.6}$$

$$E_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} E_k(x)y^{n-k}. \tag{6.7}$$

Lemma 6.1.1 *For any integer $n > 0$,*

$$\sum_{i=0}^{n} \binom{n}{i} (-i)^{[n-1]} = 2(-1)^{n-1}n!.$$

Proof. Since $(-i)^{[n-1]} = 0$ when $0 \le i \le n-2$, we have

$$\sum_{i=0}^{n} \binom{n}{i} (-i)^{[n-1]} = \binom{n}{n-1} (1-n)^{[n-1]} + \binom{n}{n} (-n)^{[n-1]} = 2(-1)^{n-1} n!. \quad \blacksquare$$

Lemma 6.1.2 *For any integer $n \ge 0$,*

$$-2nx^{n-1} + \sum_{i=1}^{n} x^{n-i} E_{i-1}(x) = \sum_{i=1}^{n} (-1)^i x^{n-i} E_{i-1}(-x).$$

Proof. Using (6.6), we have

$$E_{i-1}(-x) = (-1)^{i-1}(2x^{i-1} - E_{i-1}(x))$$

so

$$(-1)^i x^{n-i} E_{i-1}(-x) = -2x^{n-1} + x^{n-i} E_{i-1}(x).$$

Therefore,

$$\sum_{i=1}^{n} (-1)^i x^{n-i} E_{i-1}(-x) = -2nx^{n-1} + \sum_{i=1}^{n} x^{n-i} E_{i-1}(x). \quad \blacksquare$$

Lemma 6.1.3 *For any integer $n \ge 0$,*

$$\sum_{i=1}^{n} \binom{n}{i} x^{n-i} E_{i-1}(0) = \sum_{i=1}^{n} x^{n-i} E_{i-1}(x).$$

Proof. Let

$$z_n = \sum_{i=1}^{n} \binom{n}{i} x^{n-i} E_{i-1}(0);$$

then

$$\begin{aligned} z_n &= \sum_{i=1}^{n-1} \binom{n-1}{i} x^{n-i} E_{i-1}(0) + \sum_{i=1}^{n} \binom{n-1}{i-1} x^{n-i} E_{i-1}(0) \\ &= x \sum_{i=1}^{n-1} \binom{n-1}{i} x^{n-1-i} E_{i-1}(0) + \sum_{j=0}^{n-1} \binom{n-1}{j} x^{n-1-j} E_j(0) \\ &= x z_{n-1} + \sum_{j=0}^{n-1} \binom{n-1}{j} x^{n-1-j} E_j(0). \end{aligned}$$

By (6.7),

$$z_n = x z_{n-1} + E_{n-1}(x).$$

Therefore,

$$\frac{E_{n-1}(x)}{x^n} = \frac{z_n}{x^n} - \frac{z_{n-1}}{x^{n-1}}$$

and

$$\sum_{i=1}^{n} \frac{E_{i-1}(x)}{x^i} = \frac{z_n}{x^n} - z_0 = \frac{z_n}{x^n}.$$

It follows that

$$z_n = \sum_{i=1}^{n} x^{n-i} E_{i-1}(x). \quad \blacksquare$$

6.2 Convolution alternating power sums

Let $T_i(n)$ denote the alternating power sum

$$T_i(n) = \sum_{k=0}^{n} (-1)^k k^i,$$

with the convention that $0^0 = 1$. In this section, we define the *convolution alternating power sum* $T_{i,j}(n)$ as follows

Definition 6.2.1 *For any integers $i, j \geq 0$, define the following convolution alternating power sum*

$$T_{i,j}(n) = \sum_{k=0}^{n} (-1)^k k^i (n-k)^j.$$

We will give explicit formulas for the convolution alternating power sums based on the alternating power sums as well as on the Euler polynomials. Using the convolution alternating power sum, we establish some limit theorems involving convolution summations of alternating powers and rising factorials. These limit results will be used later to calculate the limit values of the harmonic continued fractions.

The alternating power sum can be determined based on the Euler polynomials as follows [1], [14]:

$$T_i(n) = \frac{(-1)^n E_i(n+1) + E_i(0)}{2}, \forall n, i \geq 0. \tag{6.8}$$

Motivated by the example of $T_i(n)$, we define:

Definition 6.2.2 *$P(n)$ is called an* **alternating polynomial** *if it has the form*

$$P(n) = f(n) + (-1)^n g(n)$$

where $f(n)$ and $g(n)$ are two polynomials in variable n. In this case, the notations $P^+(n)$ and $P^-(n)$ are used to denote $f(n)$ and $g(n)$, respectively.

Remark that if $P(n)$ is an alternating polynomial, then $P^+(n)$ and $P^-(n)$ are uniquely determined by $P(n)$. (In other contexts, the terminology "alternating polynomial" refers to polynomials in several variables which change sign when two variables are interchanged.)

6.2.1 Some algebraic identities

Theorem 6.2.1 *For any integers $i, j \geq 0$,*

$$\begin{aligned} T_{j,i}(n) &= (-1)^n\ T_{i,j}(n), \\ T^+_{j,i}(n) &= T^-_{i,j}(n). \end{aligned}$$

Proof. We have

$$\begin{aligned} T_{i,j}(n) &= \sum_{k=0}^{n}(-1)^k k^i (n-k)^j = \sum_{k=0}^{n}(-1)^{n-k}(n-k)^i k^j \\ &= (-1)^n \sum_{k=0}^{n}(-1)^k k^j (n-k)^i \\ &= (-1)^n\ T_{j,i}(n), \end{aligned}$$

thus,

$$\begin{aligned} T^+_{i,j}(n) + (-1)^n\ T^-_{i,j}(n) &= (-1)^n \left(T^+_{j,i}(n) + (-1)^n\ T^-_{j,i}(n)\right) \\ &= T^-_{j,i}(n) + (-1)^n\ T^+_{j,i}(n), \end{aligned}$$

and it follows that $T^+_{j,i}(n) = T^-_{i,j}(n)$ and $T^-_{j,i}(n) = T^+_{i,j}(n)$. ■

The following theorem shows how to calculate the convolution alternating power sum $T_{i,j}(n)$ in term of the alternating power sum $T_i(n)$.

Theorem 6.2.2 *For any integers $i, j \geq 0$, $T_{i,j}(n)$ is an alternating polynomial and*

$$T_{i,j}(n) = \sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k} n^k T_{i+j-k}(n).$$

Proof. We have

$$\begin{aligned} T_{i,j}(n) &= \sum_{k=0}^{n}(-1)^k k^i (n-k)^j = \sum_{k=0}^{n}(-1)^k k^i \sum_{\ell=0}^{j}\binom{j}{\ell} n^\ell (-k)^{j-\ell} \\ &= \sum_{\ell=0}^{j}(-1)^{j-\ell}\binom{j}{\ell} n^\ell \sum_{k=0}^{n}(-1)^k k^{i+j-\ell} \\ &= \sum_{\ell=0}^{j}(-1)^{j-\ell}\binom{j}{\ell} n^\ell T_{i+j-\ell}(n), \end{aligned}$$

and since each $T_{i+j-\ell}(n)$ is an alternating polynomial, $T_{i,j}(n)$ is also an alternating polynomial. ■

The following theorem shows how to calculate the convolution alternating power sum $T_{i,j}(n)$ in term of the Euler polynomial values $E_i(0)$.

Theorem 6.2.3 *For any integers $i, j \geq 0$,*

$$T_{i,j}(n) = \frac{1}{2}\left(\sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k} n^k E_{i+j-k}(0) + (-1)^n \sum_{k=0}^{i}(-1)^{i-k}\binom{i}{k} n^k E_{i+j-k}(0)\right).$$

Proof. By Theorem 6.2.2,

$$T_{i,j}(n) = \sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k} n^k T_{i+j-k}(n).$$

Using the relation (6.8) between the alternating power sums and the Euler polynomials, we have

$$T_{i,j}(n) = \sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k} n^k \frac{(-1)^n E_{i+j-k}(n+1) + E_{i+j-k}(0)}{2}.$$

It follows that

$$T^+_{i,j}(n) = \frac{1}{2}\sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k} n^k E_{i+j-k}(0).$$

Applying the above formula for $T^+_{j,i}(n)$ and using Theorem 6.2.1, we have

$$T^-_{i,j}(n) = T^+_{j,i}(n) = \frac{1}{2}\sum_{k=0}^{i}(-1)^{i-k}\binom{i}{k} n^k E_{i+j-k}(0).$$

Therefore,

$$\begin{aligned} T_{i,j}(n) &= T^{+}_{i,j}(n) + (-1)^n T^{-}_{i,j}(n) \\ &= \frac{1}{2}\left(\sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k}n^k E_{i+j-k}(0) + (-1)^n \sum_{k=0}^{i}(-1)^{i-k}\binom{i}{k}n^k E_{i+j-k}(0)\right). \quad \blacksquare \end{aligned}$$

The following two theorems, which follow immediately from Theorem 6.2.3, show the asymptotic value of the convolution alternating power sum $T_{i,j}(n)$ as $n \to \infty$.

Theorem 6.2.4 *For any integers $i, j \geq 0$,*

$$\lim_{n\to\infty} \frac{T_{i,j}(n)}{n^{\max(i,j)+1}} = 0.$$

Theorem 6.2.5 *For any integers $j > i \geq 0$,*

$$\lim_{n\to\infty} \frac{T_{i,j}(n)}{n^j} = \frac{1}{2}E_i(0).$$

6.2.2 Some limit theorems

Theorem 6.2.6 *For any integers $j > i \geq 0$ and any complex number c,*

$$\lim_{n\to\infty} \frac{1}{n^j}\sum_{k=0}^{n}(-1)^k k^i (n-k+c)^{[j]} = \frac{1}{2}E_i(0).$$

Proof. We can write

$$(n-k+c)^{[j]} = (n-k)^j + c_{j-1}(n-k)^{j-1} + c_{j-2}(n-k)^{j-2} + \cdots + c_1(n-k) + c_0$$

for some complex numbers $c_{j-1}, c_{j-2}, \ldots, c_1, c_0$ depending on c. Therefore,

$$\sum_{k=0}^{n}(-1)^k k^i (n-k+c)^{[j]} = T_{i,j}(n) + c_{j-1}T_{i,j-1}(n) + c_{j-2}T_{i,j-2}(n) + \cdots + c_1 T_{i,1}(n) + c_0 T_{i,0}(n).$$

Since $i < j$, by Theorem 6.2.4 and Theorem 6.2.5,

$$\lim_{n\to\infty} \frac{1}{n^j}\sum_{k=0}^{n}(-1)^k k^i (n-k+c)^{[j]} = \lim_{n\to\infty} \frac{1}{n^j} T_{i,j}(n) = \frac{1}{2}E_i(0). \quad \blacksquare$$

Theorem 6.2.7 *For any integer $i \geq 0$ and any complex number c,*

$$\lim_{n\to\infty} \frac{1}{n^{i+1}} \sum_{k=1}^{n} (-1)^k (n-k+c)^{[i]} = 0.$$

Proof. The statement is clearly true for $i = 0$. For $i > 0$, it follows from Theorem 6.2.6. ■

Theorem 6.2.8 *For any integer $i \geq 0$ and any complex number c,*

$$\lim_{n\to\infty} \frac{1}{n^{i}} \sum_{k=1}^{n} \frac{(-1)^k}{k} (n-k+c)^{[i]} = -\ln 2.$$

Proof. We prove the result by induction on i. With $i = 0$, it is a well-known identity:

$$\sum_{k=1}^{\infty} \frac{(-1)^k}{k} = -\ln 2.$$

Assuming the hypothesis for i, we are proving the $i+1$ case. We have

$$\sum_{k=1}^{n} \frac{(-1)^k}{k} (n-k+c)^{[i+1]} = \sum_{k=1}^{n} \frac{(-1)^k}{k} (n-k+c)(n-k+c+1)^{[i]}$$

$$= (n+c) \sum_{k=1}^{n} \frac{(-1)^k}{k} (n-k+c+1)^{[i]} - \sum_{k=1}^{n} (-1)^k (n-k+c+1)^{[i]},$$

so

$$\lim_{n\to\infty} \frac{1}{n^{i+1}} \sum_{k=1}^{n} \frac{(-1)^k}{k} (n-k+c)^{[i+1]}$$
$$= \lim_{n\to\infty} \frac{n+c}{n} \frac{1}{n^i} \sum_{k=1}^{n} \frac{(-1)^k}{k} (n-k+c+1)^{[i]} - \lim_{n\to\infty} \frac{1}{n^{i+1}} \sum_{k=1}^{n} (-1)^k (n-k+c+1)^{[i]}$$
$$= -\ln 2 - 0$$

by the induction hypothesis for i and by Theorem 6.2.7. ■

Theorem 6.2.9 *For any integers $0 \leq \alpha \leq \beta$, any integer ℓ, and any complex numbers c, d,*

$$\lim_{n\to\infty} \frac{1}{n^{\beta}} \sum_{k=1}^{n+\ell} (-1)^k \frac{(k+c)^{[\alpha]} (n-k+d)^{[\beta]}}{k} = -c^{[\alpha]} \ln 2 + \frac{(-1)^{\alpha}}{2} \sum_{j=1}^{\alpha} \sum_{i=1}^{j} s_1(\alpha, j) (-c)^{j-i} E_{i-1}(-c).$$

In particular, the limit is independent of d.

Proof. Note that when $|k-n| \leq |\ell|$, the summands

$$(-1)^k \frac{(k+c)^{[\alpha]}(n-k+d)^{[\beta]}}{k} = O(n^{\alpha-1}),$$

so we can ignore these summands when we calculate the limit.

Using (6.2), we have

$$\begin{aligned}(k+c)^{[\alpha]} &= \sum_{j=0}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} (k+c)^j = \sum_{j=0}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} \sum_{i=0}^{j} \binom{j}{i} c^{j-i}k^i \\ &= \sum_{j=0}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} c^j + \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} \sum_{i=1}^{j} \binom{j}{i} c^{j-i}k^i \\ &= c^{[\alpha]} + \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} \sum_{i=1}^{j} \binom{j}{i} c^{j-i}k^i.\end{aligned}$$

Therefore,

$$\begin{aligned}&\sum_{k=1}^{n}(-1)^k \frac{(k+c)^{[\alpha]}(n-k+d)^{[\beta]}}{k} \\ &= c^{[\alpha]} \sum_{k=1}^{n}(-1)^k \frac{(n-k+d)^{[\beta]}}{k} + \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} \sum_{i=1}^{j} \binom{j}{i} c^{j-i} \sum_{k=1}^{n}(-1)^k k^{i-1}(n-k+d)^{[\beta]}.\end{aligned}$$

We want to use Theorem 6.2.6, so in the second summation, we need to change the range of k from 0 to n as

$$\begin{aligned}\sum_{k=1}^{n}(-1)^k \frac{(k+c)^{[\alpha]}(n-k+d)^{[\beta]}}{k} &= c^{[\alpha]} \sum_{k=1}^{n}(-1)^k \frac{(n-k+d)^{[\beta]}}{k} \\ &+ \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} \sum_{i=1}^{j} \binom{j}{i} c^{j-i} \sum_{k=0}^{n}(-1)^k k^{i-1}(n-k+d)^{[\beta]} - \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} jc^{j-1}(n+d)^{[\beta]}.\end{aligned}$$

By Theorem 6.2.6 and Theorem 6.2.8, we have

$$\lim_{n\to\infty} \frac{1}{n^\beta} \sum_{k=1}^{n}(-1)^k \frac{(k+c)^{[\alpha]}(n-k+d)^{[\beta]}}{k} = -c^{[\alpha]} \ln 2 + \frac{1}{2} \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} \sum_{i=1}^{j} \binom{j}{i} c^{j-i} E_{i-1}(0) - \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} jc^{j-1}.$$

By Lemma 6.1.3,

$$\lim_{n\to\infty} \frac{1}{n^\beta} \sum_{k=1}^{n}(-1)^k \frac{(k+c)^{[\alpha]}(n-k+d)^{[\beta]}}{k} = -c^{[\alpha]} \ln 2 + \frac{1}{2} \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} \sum_{i=1}^{j} c^{j-i} E_{i-1}(c) - \sum_{j=1}^{\alpha} \begin{bmatrix}\alpha\\ j\end{bmatrix} jc^{j-1}.$$

By Lemma 6.1.2,

$$\lim_{n\to\infty}\frac{1}{n^\beta}\sum_{k=1}^{n}(-1)^k\frac{(k+c)^{[\alpha]}(n-k+d)^{[\beta]}}{k}=-c^{[\alpha]}\ \ln 2+\frac{1}{2}\sum_{j=1}^{\alpha}\begin{bmatrix}\alpha\\ j\end{bmatrix}\sum_{i=1}^{j}(-1)^i c^{j-i}E_{i-1}(-c).$$

Using (6.4), we have

$$\begin{aligned}&\lim_{n\to\infty}\frac{1}{n^\beta}\sum_{k=1}^{n}(-1)^k\frac{(k+c)^{[\alpha]}(n-k+d)^{[\beta]}}{k}\\ &=-c^{[\alpha]}\ \ln 2+\frac{1}{2}\sum_{j=1}^{\alpha}(-1)^{\alpha+j}s_1(\alpha,j)\sum_{i=1}^{j}(-1)^i c^{j-i}E_{i-1}(-c)\\ &=-c^{[\alpha]}\ \ln 2+\frac{(-1)^\alpha}{2}\sum_{j=1}^{\alpha}s_1(\alpha,j)\sum_{i=1}^{j}(-c)^{j-i}E_{i-1}(-c).\quad\blacksquare\end{aligned}$$

6.3 Euler polynomials and Stirling numbers

The main result of this section, Theorem 6.3.1, is an identity involving Euler polynomials and Stirling numbers. We derive this identity by using Stirling transforms of sequences. In Theorem 6.6.1, we will use the identity to simplify the value of the harmonic continued fraction.

First, we prove the following two auxiliary lemmas.

Lemma 6.3.1 *Let*

$$U_a(x)=2(x+2)^a\ln\frac{2(x+1)}{x+2};$$

then

$$U_a^{(a-1)}(0)=4a!\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{2\lfloor\frac{a}{2}\rfloor}\right).$$

Proof. By the Leibniz differentiation formula,

$$\begin{aligned}U_a^{(a-1)}(x)&=2\left((x+2)^a\right)^{(a-1)}\ln\frac{2(x+1)}{x+2}+2\sum_{i=1}^{a-1}\binom{a-1}{i}\left((x+2)^a\right)^{(a-1-i)}\left(\ln\frac{2(x+1)}{x+2}\right)^{(i)}\\ &=2\left((x+2)^a\right)^{(a-1)}\ln\frac{2(x+1)}{x+2}+2\sum_{i=1}^{a-1}\binom{a-1}{i}\left(\frac{a!}{(i+1)!}(x+2)^{i+1}\right)\left((-1)^{i-1}(i-1)!((x+1)^{-i}-(x+2)^{-i})\right),\end{aligned}$$

so

$$U_a^{(a-1)}(0)=2\sum_{i=1}^{a-1}\binom{a-1}{i}\left(\frac{a!}{(i+1)!}2^{i+1}\right)\left((-1)^{i-1}(i-1)!(1-2^{-i})\right)=4a!\sum_{i=1}^{a-1}\binom{a-1}{i}\frac{(-1)^i-(-2)^i}{i(i+1)}.$$

If

$$x_a = \sum_{i=1}^{a-1} \binom{a-1}{i} \frac{(-1)^i - (-2)^i}{i(i+1)}$$

then it suffices to prove that

$$x_a = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{2\lfloor \frac{a}{2} \rfloor}.$$

Indeed, we have

$$\begin{aligned}
x_{a+1} - x_a &= \frac{(-1)^a - (-2)^a}{a(a+1)} + \sum_{i=1}^{a-1} \left(\binom{a}{i} - \binom{a-1}{i} \right) \frac{(-1)^i - (-2)^i}{i(i+1)} \\
&= \frac{(-1)^a - (-2)^a}{a(a+1)} + \sum_{i=1}^{a-1} \binom{a-1}{i-1} \frac{(-1)^i - (-2)^i}{i(i+1)} = \sum_{i=1}^{a} \binom{a-1}{i-1} \frac{(-1)^i - (-2)^i}{i(i+1)} \\
&= \frac{1}{a(a+1)} \sum_{i=1}^{a} \binom{a+1}{i+1} ((-1)^i - (-2)^i) \\
&= \frac{1}{a(a+1)} \left(-\sum_{i=1}^{a} \binom{a+1}{i+1} (-1)^{i+1} + \frac{1}{2} \sum_{i=1}^{a} \binom{a+1}{i+1} (-2)^{i+1} \right) \\
&= \frac{1}{a(a+1)} \left(-\left(a + \sum_{i=-1}^{a} \binom{a+1}{i+1} (-1)^{i+1} \right) + \frac{1}{2} \left(2a + 1 + \sum_{i=-1}^{a} \binom{a+1}{i+1} (-2)^{i+1} \right) \right) \\
&= \frac{1}{a(a+1)} \left(-a + \frac{1}{2} \left(2a + 1 + (-1)^{a+1} \right) \right) = \frac{1 + (-1)^{a+1}}{2a(a+1)}
\end{aligned}$$

so

$$x_{a+1} - x_a = \begin{cases} 0 & \text{if } a \text{ is even} \\ \frac{1}{a} - \frac{1}{a+1} & \text{if } a \text{ is odd} \end{cases}.$$

Since $x_0 = x_1 = 0$, we have

$$x_a = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{2\lfloor \frac{a}{2} \rfloor}. \quad \blacksquare$$

Lemma 6.3.2 *Let*

$$W_a(x) = 2(e^x + 1)^a \ln \frac{2e^x}{e^x + 1};$$

then

$$W_a^{(j)}(0) = \sum_{\alpha=0}^{a} \sum_{i=1}^{j} \binom{a}{\alpha} \binom{j}{i} \alpha^{j-i} E_{i-1}(0).$$

Proof. Using (6.5), we have

$$\frac{2}{e^x + 1} = \sum_{i=0}^{\infty} \frac{E_i(0)}{i!} x^i.$$

Integrating both sides we have

$$\sum_{i=1}^{\infty} \frac{E_{i-1}(0)}{i!} x^i = \int_x \frac{2}{e^x+1} = 2(x - \ln(e^x+1)) + C.$$

Making both sides of the above equation equal at $x = 0$, we have

$$\sum_{i=1}^{\infty} \frac{E_{i-1}(0)}{i!} x^i = 2(x - \ln(e^x+1) + \ln 2) = 2 \ln \frac{2e^x}{e^x+1}.$$

On the other hand, we have

$$(e^x+1)^a = \sum_{\alpha=0}^{a} \binom{a}{\alpha} e^{\alpha x} = \sum_{\alpha=0}^{a} \binom{a}{\alpha} \sum_{i=0}^{\infty} \frac{(\alpha x)^i}{i!} = \sum_{i=0}^{\infty} \left(\sum_{\alpha=0}^{a} \binom{a}{\alpha} \frac{\alpha^i}{i!} \right) x^i,$$

so

$$W_a(x) = 2(e^x+1)^a \ln \frac{2e^x}{e^x+1} = \sum_{i=1}^{\infty} \frac{E_{i-1}(0)}{i!} x^i \times \sum_{i=0}^{\infty} \left(\sum_{\alpha=0}^{a} \binom{a}{\alpha} \frac{\alpha^i}{i!} \right) x^i.$$

Considering the coefficient of x^j of the above series we have

$$\frac{W_a^{(j)}(0)}{j!} = \sum_{i=1}^{j} \frac{E_{i-1}(0)}{i!} \sum_{\alpha=0}^{a} \binom{a}{\alpha} \frac{\alpha^{j-i}}{(j-i)!},$$

therefore,

$$W_a^{(j)}(0) = \sum_{\alpha=0}^{a} \sum_{i=1}^{j} \binom{a}{\alpha} \binom{j}{i} \alpha^{j-i} E_{i-1}(0). \quad \blacksquare$$

The Stirling transform of a sequence $\{u_n\}_{n\geq 1}$ of numbers is the sequence $\{w_n\}_{n\geq 1}$ given by

$$w_n = \sum_{j=1}^{n} s_2(n,j) u_j.$$

The inverse transform is

$$u_n = \sum_{j=1}^{n} s_1(n,j) w_j.$$

If

$$U(x) = \sum_{n=1}^{\infty} \frac{u_n}{n!} x^n$$

is a formal power series, and

$$W(x) = \sum_{n=1}^{\infty} \frac{w_n}{n!} x^n$$

with u_n and w_n as above, then

$$W(x) = U(e^x - 1).$$

We can now prove the identity referred to above.

Theorem 6.3.1

$$\sum_{j=1}^{a-1} \sum_{\alpha=0}^{a} \sum_{i=1}^{j} s_1(a-1,j) \binom{a}{\alpha} \binom{j}{i} \alpha^{j-i} E_{i-1}(0) = 4a! \left(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{2\lfloor \frac{a}{2} \rfloor}\right).$$

Proof. Let

$$U_a(x) = 2(x+2)^a \ln \frac{2(x+1)}{x+2},$$

$$W_a(x) = 2(e^x+1)^a \ln \frac{2e^x}{e^x+1};$$

then

$$U_a(0) = W_a(0) = 0 \text{ and } W_a(x) = U_a(e^x - 1).$$

Hence, the Stirling transform of the sequence $\{U_a^{(n)}(0)\}_{n\geq 1}$ is the sequence $\{W_a^{(n)}(0)\}_{n\geq 1}$. It follows that

$$U_a^{(n)}(0) = \sum_{j=1}^{n} s_1(n,j) W_a^{(j)}(0).$$

In particular, when $n = a - 1$, we have

$$U_a^{(a-1)}(0) = \sum_{j=1}^{a-1} s_1(a-1,j) W_a^{(j)}(0).$$

This is the desired identity as in Lemma 6.3.1 it is shown that

$$U_a^{(a-1)}(0) = 4a! \left(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{2\lfloor \frac{a}{2} \rfloor}\right)$$

and in Lemma 6.3.2 it is shown that

$$W_a^{(j)}(0) = \sum_{\alpha=0}^{a} \sum_{i=1}^{j} \binom{a}{\alpha} \binom{j}{i} \alpha^{j-i} E_{i-1}(0). \quad \blacksquare$$

6.4 Closed form formula for the convergent: the general case $t \in \mathbb{R}^+$

In this section, we consider the harmonic continued fraction $HCF(t)$ where $t > 0$ is a fixed and arbitrary real number. The main results, Theorem 6.4.2 and Theorem 6.4.3, give us the closed form formulas for the numerator and the denominator of the convergents.

Theorem 6.4.1 *Let*

$$P(x) = \sum_{n=0}^{\infty} p_{n-1}x^n,$$

$$Q(x) = \sum_{n=0}^{\infty} q_{n-1}x^n.$$

Then

$$P(x) = (1+x)^{\frac{t}{2}-1}(1-x)^{-\frac{t}{2}-1},$$

$$Q(x) = (1+x)^{\frac{t}{2}-1}(1-x)^{-\frac{t}{2}-1}\int_0^x (1-u)^{\frac{t}{2}}(1+u)^{-\frac{t}{2}}du.$$

Proof. In this proof, $P(x)$ and $Q(x)$ are considered as formal power series [32] and their integration and derivative are well-defined. From the Euler-Wallis recurrence formula

$$p_n = \frac{t}{n+1}p_{n-1} + p_{n-2}, \forall n \geq 0,$$

we have

$$\sum_{n=0}^{\infty} p_n x^{n+1} = t\sum_{n=0}^{\infty} p_{n-1}\frac{x^{n+1}}{n+1} + \sum_{n=0}^{\infty} p_{n-2}x^{n+1}.$$

Therefore, for some constant C, we have

$$P(x) - p_{-1} = t\left(\int P(x)dx + C\right) + \left(p_{-2}x + x^2P(x)\right).$$

Taking derivatives, we have

$$P'(x) = tP(x) + p_{-2} + x^2P'(x) + 2xP(x)$$

and we obtain the following first-order ODE

$$P'(x) - \frac{2x+t}{1-x^2}P(x) = p_{-2}\ \frac{1}{1-x^2}.$$

The integrating factor of this ODE is

$$e^{\int -\frac{2x+t}{1-x^2}dx} = e^{\int \left(\frac{-2x}{1-x^2} - \frac{t}{2}\left(\frac{1}{1+x}+\frac{1}{1-x}\right)\right)dx} = e^{\ln(1-x^2)+\frac{t}{2}(\ln(1-x)-\ln(1+x))} = (1-x)^{\frac{t}{2}+1}(1+x)^{-\frac{t}{2}+1}.$$

Hence,

$$\frac{d}{dx}\left((1-x)^{\frac{t}{2}+1}(1+x)^{-\frac{t}{2}+1}P(x)\right) = p_{-2}(1-x)^{\frac{t}{2}}(1+x)^{-\frac{t}{2}}$$

and

$$(1-x)^{\frac{t}{2}+1}(1+x)^{-\frac{t}{2}+1}P(x) = p_{-2}\int (1-x)^{\frac{t}{2}}(1+x)^{-\frac{t}{2}}dx + C.$$

Since $p_{-2} = 0$ and $P(0) = p_{-1} = 1$, we have

$$(1-x)^{\frac{t}{2}+1}(1+x)^{-\frac{t}{2}+1}P(x) = 1.$$

Therefore,

$$P(x) = (1+x)^{\frac{t}{2}-1}(1-x)^{-\frac{t}{2}-1}.$$

Similarly,

$$(1-x)^{\frac{t}{2}+1}(1+x)^{-\frac{t}{2}+1}Q(x) = q_{-2}\int (1-x)^{\frac{t}{2}}(1+x)^{-\frac{t}{2}}dx + C.$$

Since $Q(0) = q_{-1} = 0$ and $q_{-2} = 1$,

$$(1-x)^{\frac{t}{2}+1}(1+x)^{-\frac{t}{2}+1}Q(x) = \int_0^x (1-u)^{\frac{t}{2}}(1+u)^{-\frac{t}{2}}du,$$

and we obtain

$$Q(x) = (1+x)^{\frac{t}{2}-1}(1-x)^{-\frac{t}{2}-1}\int_0^x (1-u)^{\frac{t}{2}}(1+u)^{-\frac{t}{2}}du. \quad \blacksquare$$

Now apply above to find formulas for p_n and q_n.

Theorem 6.4.2

$$p_n = \frac{1}{(n+1)!}\sum_{k=0}^{n+1}\binom{n+1}{k}\left(\frac{t}{2}-1\right)_{[k]}\left(\frac{t}{2}+1\right)^{[n+1-k]}.$$

Proof. By Theorem 6.4.1,

$$P(x) = (1+x)^{\frac{t}{2}-1}(1-x)^{-\frac{t}{2}-1},$$

so by the Leibniz differentiation formula,

$$\begin{aligned}P^{(n)}(x) &= \sum_{k=0}^{n}\binom{n}{k}\left((1+x)^{\frac{t}{2}-1}\right)^{(k)}\left((1-x)^{-\frac{t}{2}-1}\right)^{(n-k)}\\ &= \sum_{k=0}^{n}\binom{n}{k}\left(\frac{t}{2}-1\right)_{[k]}(1+x)^{\frac{t}{2}-1-k}\left(-\frac{t}{2}-1\right)_{[n-k]}(-1)^{n-k}(1-x)^{-\frac{t}{2}-1-(n-k)}\\ &= \sum_{k=0}^{n}\binom{n}{k}\left(\frac{t}{2}-1\right)_{[k]}(1+x)^{\frac{t}{2}-1-k}\left(\frac{t}{2}+1\right)^{[n-k]}(1-x)^{-\frac{t}{2}-1-(n-k)}\end{aligned}$$

and

$$P^{(n)}(0) = \sum_{k=0}^{n}\binom{n}{k}\left(\frac{t}{2}-1\right)_{[k]}\left(\frac{t}{2}+1\right)^{[n-k]}. \tag{6.9}$$

Therefore,

$$p_{n-1} = \frac{1}{n!}P^{(n)}(0) = \frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}\left(\frac{t}{2}-1\right)_{[k]}\left(\frac{t}{2}+1\right)^{[n-k]}. \quad \blacksquare$$

Theorem 6.4.3

$$q_n = \frac{1}{(n+1)!}\sum_{k=0}^{n}\sum_{u=0}^{k}\sum_{v=0}^{n-k}(-1)^k\binom{n+1}{k+1}\binom{k}{u}\binom{n-k}{v}\left(\frac{t}{2}\right)_{[u]}\left(\frac{t}{2}\right)^{[k-u]}\left(\frac{t}{2}-1\right)_{[v]}\left(\frac{t}{2}+1\right)^{[n-k-v]}.$$

Proof. By Theorem 6.4.1,

$$Q(x) = (1+x)^{\frac{t}{2}-1}(1-x)^{-\frac{t}{2}-1}\int_0^x (1-u)^{\frac{t}{2}}(1+u)^{-\frac{t}{2}}du = P(x)\int_0^x R(u)du \tag{6.10}$$

where

$$R(x) = (1-x)^{\frac{t}{2}}(1+x)^{-\frac{t}{2}}.$$

By the Leibniz differentiation formula,

$$Q^{(n+1)}(x) = P^{(n+1)}(x)\int_0^x R(u)du + \sum_{k=0}^{n}\binom{n+1}{k+1}P^{(n-k)}(x)R^{(k)}(x),$$

so

$$Q^{(n+1)}(0) = \sum_{k=0}^{n}\binom{n+1}{k+1}P^{(n-k)}(0)R^{(k)}(0). \tag{6.11}$$

Using the Leibniz differentiation formula for $R(x)$, we have

$$\begin{aligned} R^{(k)}(x) &= \sum_{u=0}^{k} \binom{k}{u} \left((1-x)^{\frac{t}{2}}\right)^{(u)} \left((1+x)^{-\frac{t}{2}}\right)^{(k-u)} \\ &= \sum_{u=0}^{k} \binom{k}{u} (-1)^u \left(\frac{t}{2}\right)_{[u]} (1-x)^{\frac{t}{2}-u} \left(-\frac{t}{2}\right)_{[k-u]} (1+x)^{-\frac{t}{2}-(k-u)} \\ &= (-1)^k \sum_{u=0}^{k} \binom{k}{u} \left(\frac{t}{2}\right)_{[u]} \left(\frac{t}{2}\right)^{[k-u]} (1-x)^{\frac{t}{2}-u} (1+x)^{-\frac{t}{2}-(k-u)}, \end{aligned}$$

so

$$R^{(k)}(0) = (-1)^k \sum_{u=0}^{k} \binom{k}{u} \left(\frac{t}{2}\right)_{[u]} \left(\frac{t}{2}\right)^{[k-u]}. \tag{6.12}$$

Now, by (6.9), we have

$$P^{(n-k)}(0) = \sum_{v=0}^{n-k} \binom{n-k}{v} \left(\frac{t}{2}-1\right)_{[v]} \left(\frac{t}{2}+1\right)^{[n-k-v]}. \tag{6.13}$$

So substituting (6.12) and (6.13) into (6.11), we have

$$Q^{(n+1)}(0) = \sum_{k=0}^{n} \binom{n+1}{k+1} \left(\sum_{v=0}^{n-k} \binom{n-k}{v} \left(\frac{t}{2}-1\right)_{[v]} \left(\frac{t}{2}+1\right)^{[n-k-v]} \right) \left((-1)^k \sum_{u=0}^{k} \binom{k}{u} \left(\frac{t}{2}\right)_{[u]} \left(\frac{t}{2}\right)^{[k-u]} \right)$$

and the theorem follows from the fact that $Q^{(n+1)}(0) = (n+1)!\, q_n$. ■

6.5 Closed form formula for the convergent: the even case $t \in 2\mathbb{Z}^+$

Throughout this section, t is assumed to be a positive even integer and $t = 2a$. We find simplified expressions for p_n and q_n.

Theorem 6.5.1 *When $t = 2a$,*

$$p_n = \frac{1}{a!} \sum_{k=0}^{a-1} \binom{a-1}{k} (n-k+2)^{[a]}.$$

Proof. By Theorem 6.4.2,

$$p_n = \frac{1}{(n+1)!} \sum_{k=0}^{n+1} \binom{n+1}{k} (a-1)_{[k]} (a+1)^{[n+1-k]}.$$

Since the summand in the above sum is zero when $k \geq a$, it follows that,

$$\begin{aligned} p_n &= \frac{1}{(n+1)!}\sum_{k=0}^{a-1}\binom{n+1}{k}(a-1)_{[k]}(a+1)^{[n+1-k]} \\ &= \frac{1}{(n+1)!}\sum_{k=0}^{a-1}\frac{(n+1)!}{k!(n+1-k)!}\frac{(a-1)!}{(a-1-k)!}\frac{(a+1+n-k)!}{a!} \\ &= \frac{1}{a!}\sum_{k=0}^{a-1}\frac{(a-1)!}{k!(a-1-k)!}\frac{(a+1+n-k)!}{(n+1-k)!} \\ &= \frac{1}{a!}\sum_{k=0}^{a-1}\binom{a-1}{k}(n-k+2)^{[a]}. \quad \blacksquare \end{aligned}$$

Theorem 6.5.2 *When $t = 2a$,*

$$q_n = -\frac{1}{a!\,(a-1)!}\sum_{k=1}^{n+1}\sum_{u=0}^{\min(k-1,a)}\sum_{v=0}^{a-1}\binom{a}{u}\binom{a-1}{v}\frac{(-1)^k}{k}(k-u)^{[a-1]}(n-k-v+2)^{[a]}.$$

Proof. By Theorem 6.4.3, we have

$$q_n = \sum_{k=0}^{n}\sum_{u=0}^{k}\sum_{v=0}^{n-k}\mu(n,k,u,v),$$

where

$$\mu(n,k,u,v) = \frac{(-1)^k}{(n+1)!}\binom{n+1}{k+1}\binom{k}{u}\binom{n-k}{v}a_{[u]}a^{[k-u]}(a-1)_{[v]}(a+1)^{[n-k-v]}.$$

Since $\mu(n,k,u,v) = 0$ when $u \geq a+1$ and when $v \geq a$, we have

$$q_n = \sum_{k=0}^{n}\sum_{u=0}^{\min(k,a)}\sum_{v=0}^{\min(n-k,a-1)}\mu(n,k,u,v).$$

With $u \leq \min(k,a)$ and $v \leq \min(n-k, a-1)$, we have

$$\begin{aligned} &\mu(n,k,u,v) \\ &= \frac{(-1)^k}{(k+1)!(n-k)!}\frac{k!}{(k-u)!u!}\frac{(n-k)!}{(n-k-v)!v!}\frac{a!}{(a-u)!}\frac{(a-1+k-u)!}{(a-1)!}\frac{(a-1)!}{(a-1-v)!}\frac{(a+n-k-v)!}{a!} \\ &= \frac{(-1)^k}{k+1}\frac{1}{u!(a-u)!v!(a-1-v)!}\frac{(a-1+k-u)!}{(k-u)!}\frac{(a+n-k-v)!}{(n-k-v)!} \\ &= \frac{(-1)^k}{k+1}\frac{(k-u+1)^{[a-1]}(n-k-v+1)^{[a]}}{u!(a-u)!v!(a-1-v)!}. \end{aligned}$$

Since $(n-k-v+1)^{[a]}=0$ when $n-k<v\le a-1$, we have

$$\begin{aligned}q_n&=\sum_{k=0}^{n}\sum_{u=0}^{\min(k,a)}\sum_{v=0}^{a-1}\frac{(-1)^k}{k+1}\frac{(k-u+1)^{[a-1]}(n-k-v+1)^{[a]}}{u!(a-u)!v!(a-1-v)!}\\&=\sum_{k=1}^{n+1}\sum_{u=0}^{\min(k-1,a)}\sum_{v=0}^{a-1}\frac{(-1)^{k-1}}{k}\frac{(k-u)^{[a-1]}(n-k-v+2)^{[a]}}{u!(a-u)!v!(a-1-v)!}\\&=-\frac{1}{a!\,(a-1)!}\sum_{k=1}^{n+1}\sum_{u=0}^{\min(k-1,a)}\sum_{v=0}^{a-1}\binom{a}{u}\binom{a-1}{v}\frac{(-1)^k}{k}(k-u)^{[a-1]}(n-k-v+2)^{[a]}.\end{aligned}$$ ■

The following theorem is useful later to find the limit value for $HCF(t)$.

Theorem 6.5.3 *When $t=2a$, let*

$$A_n=\sum_{k=1}^{n+1}\sum_{u=0}^{a}\sum_{v=0}^{a-1}\binom{a}{u}\binom{a-1}{v}\frac{(-1)^k}{k}(k-u)^{[a-1]}(n-k-v+2)^{[a]};$$

then

$$q_n=(-1)^a p_{n-1}-\frac{A_n}{a!\,(a-1)!}.$$

Proof. By Theorem 6.5.2, we have

$$\begin{aligned}q_n&=-\frac{1}{a!\,(a-1)!}\sum_{k=1}^{n+1}\sum_{u=0}^{\min(k-1,a)}\sum_{v=0}^{a-1}\binom{a}{u}\binom{a-1}{v}\frac{(-1)^k}{k}(k-u)^{[a-1]}(n-k-v+2)^{[a]}\\&=-\frac{1}{a!\,(a-1)!}\sum_{k=1}^{n+1}\sum_{u=0}^{a}\sum_{v=0}^{a-1}\binom{a}{u}\binom{a-1}{v}\frac{(-1)^k}{k}(k-u)^{[a-1]}(n-k-v+2)^{[a]}\\&\quad+\frac{1}{a!\,(a-1)!}\sum_{k=1}^{a+1}\sum_{u=k}^{a}\sum_{v=0}^{a-1}\binom{a}{u}\binom{a-1}{v}\frac{(-1)^k}{k}(k-u)^{[a-1]}(n-k-v+2)^{[a]},\end{aligned}$$

so

$$q_n=\frac{1}{a!\,(a-1)!}(-A_n+\alpha_n),$$

where

$$\alpha_n=\sum_{k=1}^{a+1}\sum_{u=k}^{a}\sum_{v=0}^{a-1}\binom{a}{u}\binom{a-1}{v}\frac{(-1)^k}{k}(k-u)^{[a-1]}(n-k-v+2)^{[a]}.$$

When $1\le k\le a+1$ and $k\le u\le a$, $(k-u)^{[a-1]}$ is zero except for the case $k=1$

and $u = a$, therefore,

$$\alpha_n = -\sum_{v=0}^{a-1} \binom{a-1}{v} (1-a)^{[a-1]} (n+1-v)^{[a]} = (-1)^a (a-1)! \sum_{v=0}^{a-1} \binom{a-1}{v} (n+1-v)^{[a]}.$$

By Theorem 6.5.1,

$$\alpha_n = (-1)^a \, (a-1)! \, a! \, p_{n-1}.$$

Therefore,

$$q_n = (-1)^a p_{n-1} - \frac{A_n}{a! \, (a-1)!}. \quad \blacksquare$$

Theorem 6.5.4 *When $t = 2a$,*

$$\lim_{n\to\infty} \frac{p_n}{n^a} = \frac{2^{a-1}}{a!}.$$

Proof. By Theorem 6.5.1,

$$\lim_{n\to\infty} \frac{p_n}{n^a} = \frac{1}{a!} \sum_{k=0}^{a-1} \binom{a-1}{k} \lim_{n\to\infty} \frac{(n-k+2)^{[a]}}{n^a} = \frac{1}{a!} \sum_{k=0}^{a-1} \binom{a-1}{k} = \frac{2^{a-1}}{a!}. \quad \blacksquare$$

Theorem 6.5.5 *When $t = 2a$,*

$$\lim_{n\to\infty} \frac{q_n}{n^a} = (-1)^a \frac{2^{a-1}}{a!} \left(1 - 2a \ \ln 2 + \frac{1}{2 \ (a-1)!} \sum_{u=0}^{a} \sum_{j=1}^{a-1} \sum_{i=1}^{j} \binom{a}{u} s_1(a-1, j) u^{j-i} E_{i-1}(u) \right).$$

Proof. We have

$$\lim_{n\to\infty} \frac{A_n}{n^a} = \sum_{u=0}^{a} \sum_{v=0}^{a-1} \binom{a}{u} \binom{a-1}{v} A(u, v),$$

where

$$A(u, v) = \lim_{n\to\infty} \frac{1}{n^a} \sum_{k=1}^{n+1} \frac{(-1)^k}{k} (k-u)^{[a-1]} (n-k-v+2)^{[a]}.$$

By Theorem 6.2.9, $A(u, v)$ is independent of v, as

$$A(u, v) = -(-u)^{[a-1]} \ \ln 2 + \frac{(-1)^{a-1}}{2} \sum_{j=1}^{a-1} \sum_{i=1}^{j} s_1(a-1, j) u^{j-i} E_{i-1}(u) = A(u).$$

Therefore,

$$\begin{aligned}
&\lim_{n\to\infty}\frac{A_n}{n^a}\\
&=2^{a-1}\sum_{u=0}^{a}\binom{a}{u}A(u)\\
&=2^{a-1}\sum_{u=0}^{a}\binom{a}{u}\left(-(-u)^{[a-1]}\ \ln 2+\frac{(-1)^{a-1}}{2}\sum_{j=1}^{a-1}\sum_{i=1}^{j}s_1(a-1,j)u^{j-i}E_{i-1}(u)\right)\\
&=-2^{a-1}\ln 2\sum_{u=0}^{a}\binom{a}{u}(-u)^{[a-1]}-(-1)^a2^{a-2}\sum_{u=0}^{a}\sum_{j=1}^{a-1}\sum_{i=1}^{j}\binom{a}{u}s_1(a-1,j)u^{j-i}E_{i-1}(u).
\end{aligned}$$

By Lemma 6.1.1,

$$\lim_{n\to\infty}\frac{A_n}{n^a}=(-1)^a2^a a!\ln 2-(-1)^a2^{a-2}\sum_{u=0}^{a}\sum_{j=1}^{a-1}\sum_{i=1}^{j}\binom{a}{u}s_1(a-1,j)u^{j-i}E_{i-1}(u).$$

By Theorem 6.5.3,

$$\lim_{n\to\infty}\frac{q_n}{n^a}=(-1)^a\lim_{n\to\infty}\frac{p_{n-1}}{n^a}-\frac{1}{a!\,(a-1)!}\lim_{n\to\infty}\frac{A_n}{n^a}.$$

By Theorem 6.5.4,

$$\begin{aligned}
&\lim_{n\to\infty}\frac{q_n}{n^a}\\
&=(-1)^a\frac{2^{a-1}}{a!}-\frac{1}{a!\,(a-1)!}\left((-1)^a2^a a!\ln 2-(-1)^a2^{a-2}\sum_{u=0}^{a}\sum_{j=1}^{a-1}\sum_{i=1}^{j}\binom{a}{u}s_1(a-1,j)u^{j-i}E_{i-1}(u)\right)\\
&=(-1)^a\frac{2^{a-1}}{a!}\left(1-2a\ \ln 2+\frac{1}{2\ (a-1)!}\sum_{u=0}^{a}\sum_{j=1}^{a-1}\sum_{i=1}^{j}\binom{a}{u}s_1(a-1,j)u^{j-i}E_{i-1}(u)\right).\quad\blacksquare
\end{aligned}$$

6.6 Main theorem for the even case

Theorem 6.6.1 *For any positive integer a,*

$$\begin{aligned} HCF(2a) &= \frac{(-1)^{a-1}}{2a\,\ln 2 - 1 - \frac{1}{2\,(a-1)!}\sum_{u=0}^{a}\sum_{j=1}^{a-1}\sum_{i=1}^{j}\binom{a}{u}s_1(a-1,j)u^{j-i}E_{i-1}(u)} \\ &= \frac{(-1)^{a-1}}{2a\,\ln 2 - 1 - \frac{1}{2\,(a-1)!}\sum_{u=0}^{a}\sum_{j=1}^{a-1}\sum_{i=1}^{j}\binom{a}{u}s_1(a-1,j)\binom{j}{i}u^{j-i}E_{i-1}(0)} \\ &= \frac{(-1)^{a-1}}{2a\,\ln 2 - 1 - 2a\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{2\lfloor\frac{a}{2}\rfloor}\right)}. \end{aligned}$$

Proof. The first identity is by Theorem 6.5.4 and Theorem 6.5.5. The second identity is by Lemma 6.1.3. The third identity is by Theorem 6.3.1. ■

Chapter 7

Cryptanalysis of the RSA System

In this chapter, we will present an attack on the RSA cryptosystem. We show that if the public key and the private key are smaller than a certain bound then it is possible to efficiently perform the RSA number factorization and determine the private key using continued fractions.

The RSA is a public-key cryptosystem widely used for secure data transmission. The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm [37] in 1978. When we are surfing on the Internet, if the address bar starts with https://, it means that we are using a secure protocol and the data transmitted between our computer and the website's server are protected probably with the RSA encryption algorithm.

In general, a cryptosystem consists of two functions, *encrypt* and *decrypt*. The *encrypt* function uses an encryption key to transform the plaintext – such as our credit card number – into a scrambled ciphertext. Decryption is simply the inverse of encryption. The *decrypt* function uses a decryption key to transform the ciphertext back to the plaintext.

Cryptosystems are divided into two categories: symmetric and asymmetric. In a *symmetric*-key cryptosystem, the encryption key and the decryption key are the same, and the two parties in the communication need to agree on the key they are using. A typical example would be when agent James Bond of the British Secret Service MI6, before going out on field trip, would set up a key with his base. He will use this key to encrypt his messages and send them back to MI6. At the home base, the same key is used in decryption to read his messages. On the other hand, an *asymmetric*-key cryptosystem, also known as a public-key cryptosystem, uses two different keys, one public key for encryption and one private key for decryption.

The public key can be shared with everyone, whereas the private key must be kept secret. A typical example would be, in online banking, when we visit the bank's website, and the website sends its certificate which contains its public key to our computer. We can encrypt our sensitive data using the bank's public key and only the bank who has the private key can use it to decrypt our data.

Of course, an asymmetric-key cryptosystem is more convenient than a symmetric-key cryptosystem, particularly in cyberspace, since the two parties in the communication do not need to meet up to arrange a secret key. The RSA is the most widely used asymmetric algorithm on the Internet.

In a public-key cryptosystem, the public key and the private key are mathematically linked and it should be computationally impossible for anyone to determine the private key from the public key. This means that the system needs to be based on some hard computational maths problem. The RSA cryptosystem is based on the hardness of factorization of big numbers. To generate an RSA key, one would select two large prime numbers p and q, and multiply them to get a huge number $N = pq$. Next, choose two numbers $1 < e, d < (p-1)(q-1)$ such that $ed = 1 \pmod{(p-1)(q-1)}$. The public key is (N, e) and the private key is (p, q, d). A plaintext $1 < m < N$ is encrypted as $c = m^e \pmod{N}$ and the ciphertext c is decrypted as $m = c^d \pmod{N}$. The decryption and encryption cancel out each other thanks to Euler's theorem [21]:

$$m^{(p-1)(q-1)} = 1 \pmod{N}.$$

The security of the RSA is based on the hardness of factorization of big numbers. Given a huge modulus N in the public key, of order, say, 2^{1000}, there is no efficient algorithm currently available to factor N to find the two primes p and q. Thus, everyone knows N but no one knows $\phi(N) = (p-1)(q-1)$ except the owner of the key. So from the public information (N, e), it would be computationally impossible for anyone to determine the secret value $d = e^{-1} \pmod{\phi(N)}$.

The running time of the RSA encryption function depends on how large the public exponent e is. Whereas, the running time of the decryption function depends on the size of the private exponent d. In some scenarios, where the device on which the encryption or decryption taken place has limited computational resources, such as a credit card or an ATM machine, it is desirable to use relatively small parameters e or d. However, Wiener [46] showed that, using continued fractions, one can efficiently recover the secret key d from the public information (N, e) if $d < \frac{1}{3}N^{\frac{1}{4}}$ (see also [5], [31]). Exploiting a non-linear equation satisfied by the secret key, Boneh et al. [5]

presented a lattice-based attack that succeeds in polynomial-time when $d < N^{0.292}$. By using the continued fraction technique, Bunder and Tonien [10], [11] showed that the secret key can be recovered if $d^2e < 8N^{\frac{3}{2}}$. So if $e \approx N^{\alpha}$, then this method can recover the secret key if $d < 2\sqrt{2}\, N^{\frac{3}{4}-\frac{\alpha}{2}}$ and certainly for $d < 2\sqrt{2}\, N^{\frac{1}{4}}$ – which is more than 8 times the Wiener's bound.

In this chapter, we extend the work of [10], [11]. We improve the bound to

$$d^2e < 8tN^{\frac{3}{2}},$$

for an arbitrary parameter t, and the running time of our algorithm is $O(t \log N)$.

Our new attack is verified by an experiment with a 1024-bit modulus N and a 301-bit secret key d, which is out of reach for the previous attacks by Wiener [46] and Boneh et al [5]. In the following figure, the shaded part shows the area where our method is better than that of [46] and [5].

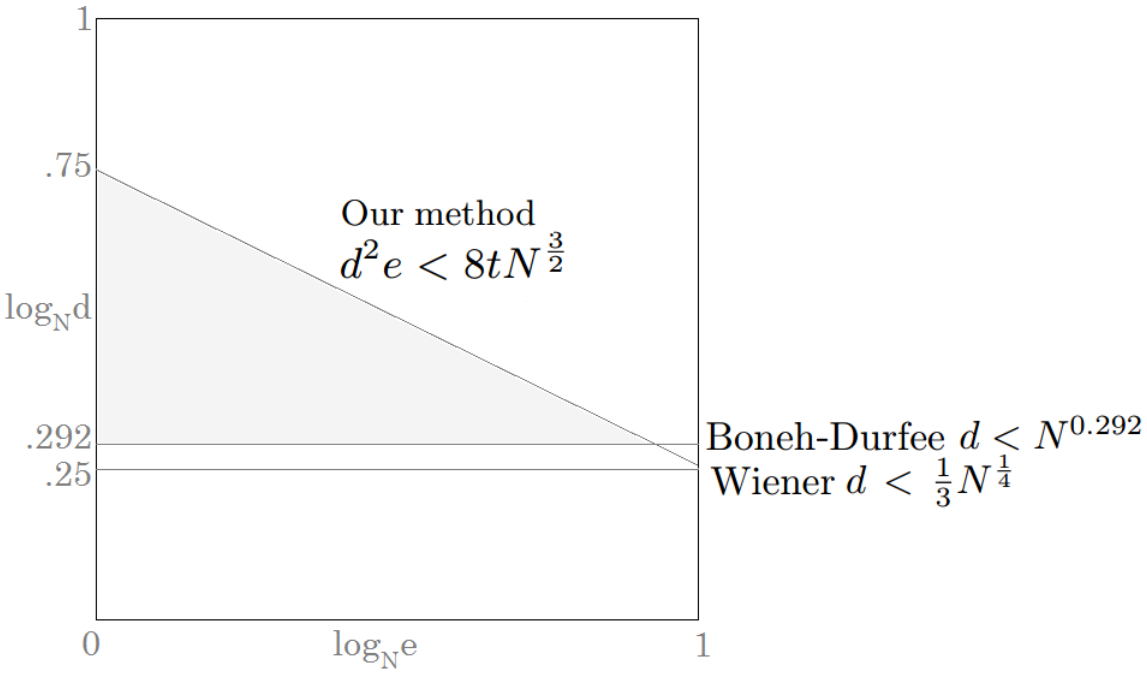

Figure 7.1: Using continued fractions, for any fixed value of $t \in \mathbb{Z}^+$, our method can determine the secret key (p, q, d) from the public key (N, e) in time complexity $O(t \log(N))$ if $d^2e < 8tN^{\frac{3}{2}}$.

7.1 The RSA algorithm

RSA is a public-key cryptosystem widely used for secure data transmission.

Key Generation:

- Choose two distinct prime numbers p and q of similar bit lengths.
- Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
- Choose $e \in (1, \phi(N))$ such that $\gcd(e, \phi(N)) = 1$ and calculate

$$d = e^{-1} \pmod{\phi(N)} \in (1, \phi(N)).$$

  Or equivalently, choose $d \in (1, \phi(N))$ such that $\gcd(d, \phi(N)) = 1$ and calculate

$$e = d^{-1} \pmod{\phi(N)}.$$

- The public key is (N, e). The private key is (p, q, d).

Encrypt function:

- For a message $m \in (1, N)$, the ciphertext c is determined as

$$c = m^e \pmod{N} \in (1, N).$$

Decrypt function:

- For a ciphertext $c \in (1, N)$, the message m is determined as

$$m = c^d \pmod{N} \in (1, N).$$

The correctness of the algorithm. Since $ed = 1 \pmod{\phi(N)}$, we have

$$ed = 1 + k\phi(N)$$

for some $k \in \mathbb{N}$, so

$$c^d = (m^e)^d = m^{ed} = m^{1+k\phi(N)} = m \cdot (m^{\phi(N)})^k = m \pmod{N}$$

and thus, the encrypt and decrypt functions cancel out each other.

Example. For an example, we choose the following two primes using the digits of $\sqrt{19}$ and the number π:

$$\begin{aligned} p = &\ \lfloor 10^5 \times \sqrt{19} \rfloor &= 435889 \\ q = &\ \lfloor 10^5 \times \pi \rfloor &= 314159, \end{aligned}$$

which give the RSA modulus

$$N = pq = 136938452351.$$

We choose the public exponent

$$e = 2017$$

and derive the private exponent

$$d = e^{-1} \pmod{\phi(N)} = 75767216545.$$

For a message

$$m = 123456789,$$

encryption gives

$$\begin{aligned} c &= m^e \pmod{N} = 123456789^{2017} \pmod{136938452351} \\ &= 60322867288. \end{aligned}$$

Decryption of this ciphertext gives back the message

$$\begin{aligned} m &= c^d \pmod{N} = 60322867288^{75767216545} \pmod{136938452351} \\ &= 123456789. \end{aligned}$$

7.2 The Wiener attack

The complexity of the decrypt function is based on the size of the decryption key d. In a cryptosystem with a limited resource such as a credit card, it is desirable to have a smaller value of d. Wiener's attack uses the continued fraction method to expose the private key d when d is small ($d < \frac{1}{3}N^{\frac{1}{4}}$).

The following theorem summarises Wiener's attack [5], [46].

Theorem 7.2.1 *If the following conditions are satisfied*

- $q < p < 2q$
- $0 < e, d < \phi(N)$
- $ed - k\phi(N) = 1$
- $\boxed{d < \frac{1}{3}N^{\frac{1}{4}}}$

then $\frac{k}{d}$ *is a convergent of the regular continued fraction of* $\frac{e}{N}$ *and there is an algorithm with time complexity* $O(\log(N))$ *that can determine the secret information* p, q, d, k *from the public key* (N, e).

Since $\frac{e}{N}$ has $O(\log(N))$ number of convergents, Wiener's algorithm will succeed to factor N and output p, q, d, k in $O(\log(N))$ time complexity.

The idea behind Wiener's attack is as follows. From the equation $ed - k\phi(N) = 1$, we have

$$\frac{e}{\phi(N)} - \frac{k}{d} = \frac{1}{d\phi(N)} \quad \text{is small.}$$

We do not know $\frac{e}{\phi(N)}$, but we know its approximation

$$\frac{e}{\phi(N)} \approx \frac{e}{N},$$

so if d is a number such that

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

then by Theorem 1.4.9, $\frac{k}{d}$ is a convergent of $\frac{e}{N}$. Thus, by calculating the continued fraction of $\frac{e}{N}$ we can discover the secret information d.

Example 1. In the following example, we have a 1024-bit modulus N, the upper bound $\frac{1}{3}N^{\frac{1}{4}}$ in Theorem 7.2.1 is 255-bit, d is 255-bit and we have found the convergent $c_{149} = \frac{p_{149}}{q_{149}} = \frac{k}{d}$ as asserted by Theorem 7.2.1.

p	12137	
	2429807756 5612551149 2629609691 9449141205 8680156593	
	9661850265 4224438815 0519802020 4979508724 3102230079	
	9409502534 6163494126 0471531617 7098769594 1320931493	512 bits
q	9201	
	0524322086 3900671386 8662660639 9738950237 2692456878	
	2613825773 8431082681 6215281513 7070448098 3908271161	
	4206768781 4447541784 7243525840 6453897707 3778553491	512 bits
N	111675409	
	0485730823 5978712392 1718417590 8091542898 6532382066	
	5485087798 8534958587 2419428390 8818158158 7258671440	
	7683378413 7900981405 8406611299 6495087782 9075022344	
	5692173775 8022280271 1775885570 7370037539 5363272503	
	0411307566 7128393688 9712399229 9533595050 1425299028	
	6693467091 9270372721 8720248761 5489260235 4246992063	1024 bits
$\phi(N)$	111675409	
	0485730823 5978712392 1718417590 8091542898 6532382066	
	5485087798 8534958587 2419428390 8818158158 7258671440	
	7683378413 7900981405 8406611299 6495087782 9075001006	
	2738043932 8509057735 0483615238 8181946096 3990659030	
	8135631527 4472872192 2977315695 7483638227 4414797787	
	3077195775 8659336811 1005191303 1936592933 9147507080	1024 bits
Theorem 7.2.1	3426637 2625316286 2968546235	
bound $\frac{1}{3}N^{\frac{1}{4}}$	7247145632 3454416288 1157194267 8892540948 5361638977	255 bits
e	45643085	
	8324017120 3133152071 1529402253 9055348712 7592566099	
	1853899212 7134329984 8723684744 2845550165 4714497720	
	7173865355 1358820024 8341016147 1746464324 1362580067	
	0745402653 2892481331 8307985083 2822164891 3129959216	
	3726940854 8355291478 1683701096 4254131032 8949699809	
	7582249761 4243019490 2375579169 7150271910 4226716997	1023 bits
d	3426637 2625316286 2968546235	
	7247145632 3454416288 1157194267 8892540948 5361638973	255 bits
k	1400507 9544612205 2131699024	
	5626308122 5492430329 4046240953 0743691100 4314600526	253 bits
convergent of $\frac{e}{N}$	found $c_{149} = \frac{p_{149}}{q_{149}} = \frac{k}{d}$	

7.3 The new attack

In this section, we present our new attack which is an improvement over the Wiener attack.

First, let us review the idea behind Wiener's attack. Since $ed - k\phi(N) = 1$, we have

$$\frac{e}{\phi(N)} - \frac{k}{d} = \frac{1}{d\phi(N)} \quad \text{is small.}$$

We do not know $\frac{e}{\phi(N)}$, but we know its approximation

$$\frac{e}{\phi(N)} \approx \frac{e}{N},$$

so if d is a number such that

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

then by Theorem 1.4.9, $\frac{k}{d}$ is a convergent of $\frac{e}{N}$. Thus, by calculating the continued fraction of $\frac{e}{N}$ we can discover the secret information d.

In our attack, instead of using the convergents of the continued fraction of $\frac{e}{N}$ as in the Wiener's original attack, we will use the convergents of the continued fraction of $\frac{e}{N'}$ where N' is a better approximation of $\phi(N)$.

We have the following observation. Consider an arbitrary interval (ϕ_{min}, ϕ_{max}) and suppose that $\phi \in (\phi_{min}, \phi_{max})$. If we divide the interval (ϕ_{min}, ϕ_{max}) into 2 equal sub-intervals with the midpoint N_1 as in Figure 7.2, then no matter where ϕ lies on the interval, we always have

$$|\phi - N_1| \leq \frac{\phi_{max} - \phi_{min}}{2}.$$

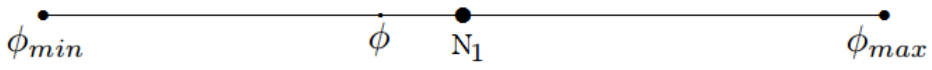

Figure 7.2: Divide the interval into 2 equal sub-intervals with midpoint N_1.

If we divide the interval (ϕ_{min}, ϕ_{max}) into 4 equal sub-intervals as in Figure 7.3 with

$$N_1 = \phi_{min} + \frac{\phi_{max} - \phi_{min}}{4} \text{ and } N_2 = \phi_{min} + 3\frac{\phi_{max} - \phi_{min}}{4},$$

then no matter where ϕ lies on the interval, we always can find N_i such that

$$|\phi - N_i| \leq \frac{\phi_{max} - \phi_{min}}{4}.$$

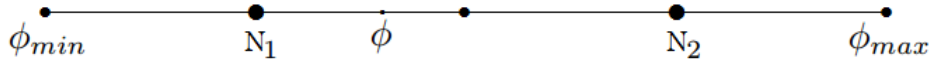

Figure 7.3: Divide the interval into 4 equal sub-intervals with $N_1 = \phi_{min} + \frac{\phi_{max}-\phi_{min}}{4}$ and $N_2 = \phi_{min} + 3\frac{\phi_{max}-\phi_{min}}{4}$.

And if we divide the interval (ϕ_{min}, ϕ_{max}) into 6 equal sub-intervals as in Figure 7.4 with

$$N_1 = \phi_{min}+\frac{\phi_{max}-\phi_{min}}{6}, N_2 = \phi_{min}+3\frac{\phi_{max}-\phi_{min}}{6} \text{ and } N_3 = \phi_{min}+5\frac{\phi_{max}-\phi_{min}}{6},$$

then we always can find N_i such that

$$|\phi - N_i| \leq \frac{\phi_{max}-\phi_{min}}{6}.$$

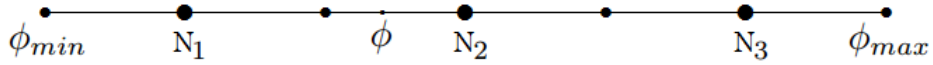

Figure 7.4: Divide the interval into 6 equal sub-intervals with $N_1 = \phi_{min} + \frac{\phi_{max}-\phi_{min}}{6}$, $N_2 = \phi_{min} + 3\frac{\phi_{max}-\phi_{min}}{6}$ and $N_3 = \phi_{min} + 5\frac{\phi_{max}-\phi_{min}}{6}$.

We have the following general result.

Lemma 7.3.1 *Suppose that $\phi \in (\phi_{min}, \phi_{max})$. Let $t \in \mathbb{N}$ be a fixed positive integer and define*

$$N_i = \phi_{min} + (2i-1)\frac{\phi_{max}-\phi_{min}}{2t}, 1 \leq i \leq t,$$

then there exists i such that

$$|\phi - N_i| \leq \frac{\phi_{max}-\phi_{min}}{2t}.$$

This is our main theorem.

Theorem 7.3.1 *Let t be a fixed positive integer. In the RSA algorithm, if the following conditions are satisfied*

- $q < p < 2q$
- $0 < e, d < \phi(N)$
- $ed - k\phi(N) = 1$
- $N > 2000000\, t^2$
- $\boxed{d^2 e < 8tN^{\frac{3}{2}}}$

and

$$N_i = N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}} + (2i-1)\frac{(\frac{3}{\sqrt{2}} - 2)N^{\frac{1}{2}}}{2t}, 1 \leq i \leq t,$$

then $\frac{k}{d}$ *is a convergent of the regular continued fraction of* $\frac{e}{\lfloor N_i \rfloor}$ *for some* $i \in [1, t]$ *and there is an algorithm with time complexity* $O(t\log(N))$ *that can determine the secret information* p, q, d, k *from the public key* (N, e).

Proof. It follows from $q < p < 2q$ that $1 < \sqrt{\frac{p}{q}} < \sqrt{2}$, so since the function $f(x) = x + \frac{1}{x}$ is increasing on $[1, +\infty)$, we have

$$2 < \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} < \sqrt{2} + \frac{1}{\sqrt{2}} = \frac{3}{\sqrt{2}}.$$

Therefore,

$$2N^{\frac{1}{2}} < p + q < \frac{3}{\sqrt{2}}N^{\frac{1}{2}}$$

and

$$N + 1 - 2N^{\frac{1}{2}} > \phi(N) = N + 1 - (p + q) > N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}.$$

Let

$$\phi_{min} = N + 1 - \frac{3}{\sqrt{2}}N^{\frac{1}{2}}, \quad \phi_{max} = N + 1 - 2N^{\frac{1}{2}}.$$

then $\phi(N) \in (\phi_{min}, \phi_{max})$. From the definition of N_i, we can see that

$$N_i = \phi_{min} + (2i-1)\frac{\phi_{max} - \phi_{min}}{2t},$$

so by Lemma 7.3.1, there exists N_i such that

$$|\phi(N) - N_i| \leq \frac{\phi_{max} - \phi_{min}}{2t}.$$

Thus,

$$|\phi(N) - \lfloor N_i \rfloor| \leq |\phi(N) - N_i| + |N_i - \lfloor N_i \rfloor| < \frac{\phi_{max} - \phi_{min}}{2t} + 1.$$

We have

$$\begin{aligned}\left|\frac{e}{\lfloor N_i\rfloor}-\frac{k}{d}\right| &= \left|\left(\frac{e}{\lfloor N_i\rfloor}-\frac{e}{\phi(N)}\right)+\left(\frac{e}{\phi(N)}-\frac{k}{d}\right)\right| = \left|\frac{e(\phi(N)-\lfloor N_i\rfloor)}{\lfloor N_i\rfloor\phi(N)}+\frac{1}{d\phi(N)}\right| \\ &= \left|\frac{e(\phi(N)-\lfloor N_i\rfloor)}{\lfloor N_i\rfloor\phi(N)}+\frac{e}{\phi(N)(k\phi(N)+1)}\right| \\ &\le \frac{e|\phi(N)-\lfloor N_i\rfloor|}{\lfloor N_i\rfloor\phi(N)}+\frac{e}{\phi(N)(k\phi(N)+1)} \\ &< \frac{e(\frac{\phi_{max}-\phi_{min}}{2t}+1)}{\phi_{min}^2}+\frac{e}{\phi_{min}^2} = \frac{e(\phi_{max}-\phi_{min}+4t)}{2t\phi_{min}^2} \\ &< \frac{e(\phi_{max}-\phi_{min}+4t)}{2t(\phi_{min}-1)^2} = \frac{e}{2t}\,\frac{(\frac{3}{\sqrt{2}}-2)N^{\frac{1}{2}}+4t}{(N-\frac{3}{\sqrt{2}}N^{\frac{1}{2}})^2}.\end{aligned}$$

It remains to show that, for $N > 2000000\,t^2$,

$$\frac{(\frac{3}{\sqrt{2}}-2)N^{\frac{1}{2}}+4t}{(N-\frac{3}{\sqrt{2}}N^{\frac{1}{2}})^2} < \frac{1}{8N^{\frac{3}{2}}} \tag{7.1}$$

and thus,

$$\left|\frac{e}{\lfloor N_i\rfloor}-\frac{k}{d}\right| < \frac{e}{16tN^{\frac{3}{2}}} < \frac{1}{2d^2},$$

which, by Theorem 1.4.9, implies that $\frac{k}{d}$ is equal a convergent $\frac{p_n}{q_n}$ of the regular continued fraction of $\frac{e}{\lfloor N_i\rfloor}$.

The inequality (7.1) is equivalent to

$$\begin{aligned} & 8N^{\frac{1}{2}}\left(\left(\frac{3}{\sqrt{2}}-2\right)N^{\frac{1}{2}}+4t\right) < \left(N^{\frac{1}{2}}-\frac{3}{\sqrt{2}}\right)^2 \\ \leftrightarrow\quad & (12\sqrt{2}-16)N+32tN^{\frac{1}{2}} < N-3\sqrt{2}N^{\frac{1}{2}}+\frac{9}{2} \\ \leftrightarrow\quad & (32t+3\sqrt{2})N^{\frac{1}{2}} < (17-12\sqrt{2})N+\frac{9}{2}.\end{aligned}$$

It suffices now to show that

$$(17-12\sqrt{2})N > (32t+3\sqrt{2})N^{\frac{1}{2}}$$

which is equivalent to

$$N^{\frac{1}{2}} > \frac{32t+3\sqrt{2}}{17-12\sqrt{2}} = (544+384\sqrt{2})t+72+51\sqrt{2}.$$

Indeed, we have

$$(544 + 384\sqrt{2})t + 72 + 51\sqrt{2} < 1088t + 145 \leq 1233t < 1000\sqrt{2}t.$$

So if $N > 2000000\,t^2$ then

$$N^{\frac{1}{2}} > 1000\sqrt{2}t > (544 + 384\sqrt{2})t + 72 + 51\sqrt{2}$$

and we obtain the desired inequality (7.1).

Now, since $\frac{k}{d}$ is equal to a convergent of the regular continued fraction of $\frac{e}{\lfloor N_i \rfloor}$, we need to go through the list of all convergents of $\frac{e}{\lfloor N_i \rfloor}$ for each $1 \leq i \leq t$ to determine the secret information p, q, d, k.

Given each convergent $c_n = \frac{p_n}{q_n}$ of $\frac{e}{\lfloor N_i \rfloor}$, by Theorem 1.4.4, $\gcd(p_n, q_n) = 1$. The equation $ed - k\phi(N) = 1$ also implies $\gcd(k, d) = 1$. So if $\frac{k}{d} = \frac{p_n}{q_n}$ then $p_n = k$ and $q_n = d$. Based on the equation $ed - k\phi(N) = 1$, it is easy to check if $p_n = k$ and $q_n = d$ or not as follows:

- Check if $eq_n - 1$ is divisible by p_n or not. If not then the convergent $c_n = \frac{p_n}{q_n} \neq \frac{k}{d}$.
- If $p_n \mid eq_n - 1$, let $\phi(N) = \frac{eq_n - 1}{p_n}$
- Calculate $S = p + q = N + 1 - \phi(N)$
- Solve the quadratic equation $x^2 - Sx + N = 0$ for p and q and check if p and q are prime numbers.

Since there are t such numbers $\frac{e}{\lfloor N_i \rfloor}$ and each of these numbers $\frac{e}{\lfloor N_i \rfloor}$ has $O(\log N)$ convergents, so the algorithm runs with time complexity $O(t \log N)$. ■

The condition $d^2 e < 8tN^{\frac{3}{2}}$ in our Theorem 7.3.1 implies that if either d or e is relatively small then the RSA algorithm can be broken. When e is relatively small, the Wiener [46] attack and the Boneh et al [5] attack cannot be applied, whereas ours can.

7.4 An experimental result

In this experiment, we use a 1024-bit modulus N. With this 1024-bit modulus, the Wiener [46] upper bound $\frac{1}{3}N^{\frac{1}{4}}$ is 255-bit and the Boneh et al [5] upper bound $N^{0.292}$ is 300-bit. Here, we show an example of a 301-bit secret key d.

p	15011	
	2271103733 6565415840 3067757190 6321456869 1431825325	
	8934337930 4220889387 6648153060 2101252338 5824008783	
	1777109693 9641425989 8182377183 5489776201 0681443971	513 bits
q	7505	
	6135551866 8282707920 1533878595 3160728434 5715912662	
	9467168965 2110444693 8324076530 1050626169 2912004391	
	5888554846 9820712994 9091188591 7744888100 5340722459	512 bits
N	112668469	
	6796041526 7971520532 0876473037 7046884372 9760286962	
	6874267967 3756539269 1189672089 9781722542 1945656382	
	5759860729 9822848396 6727797775 0084652425 6540519217	
	4340471539 2411113144 5280699866 6080080254 2666742865	
	1582206786 8333213968 4817884864 7186204199 6830773388	
	8265497642 6165255577 8066003793 3742983671 0469844689	1024 bits
e	3546 8275150449 8928214645 4839949072 3541699917	
	8541053777 8814805556 3065068030 4414979123 8328581104	
	1893345269 5958651561 5309067787 8603508234 2712088372	
	4932440491 5675387082 4436150635 7150276983 7219994359	
	5285085507 4207336971 8472035998 0686363860 0357485766	
	5921571443 5738043230 0941622668 1348247084 7659063039	976 bits
d	2 0370359763 3448608626 8445688409 3781610614	
	6839033189 2501272280 8987537625 9952667341 9734643939	301 bits
Theorem 7.3.1		
t	160000000000	
$\lfloor N_1 \rfloor$	112668469	
	6796041526 7971520532 0876473037 7046884372 9760286962	
	6874267967 3756539269 1189672089 9781722542 1945656382	
	5759860729 9822848396 6727797775 0084652425 6540496700	
	5933815978 9987895073 8645796041 4302491722 7380075132	
	4186734235 4363626867 9924887347 9194343965 0319361987	
	6873850413 4428578030 3533967491 2955055377 7378990296	1024 bits
k	641263 2807160244 6527258322	
	2705582107 8117668672 2401456947 5530868714 5037898787	252 bits
convergent of $\frac{e}{N}$	not found, $c_i \neq \frac{k}{d},\ \forall i$	
convergent of $\frac{e}{\lfloor N_1 \rfloor}$	found $c_{153} = \frac{p_{153}}{q_{153}} = \frac{k}{d}$	

This experimental result shows that our usage of continued fractions of $\frac{e}{\lfloor N_i \rfloor}$ is *essential*. If we use continued fractions of $\frac{e}{N}$ as in Wiener's original attack then no convergent c_i is found for which $c_i = \frac{k}{d}$.

Chapter 8

Cryptanalysis of RSA-variant Systems

In this chapter, we apply the continued fraction method to launch a new attack on the three RSA-variant cryptosystems. The first cryptosystem [28], proposed by Kuwakado, Koyama and Tsuruoka in 1995, is a scheme based on singular cubic curves $y^2 = x^3 + bx^2 \pmod N$ where $N = pq$ is an RSA modulus. The second cryptosystem [18], proposed by Elkamchouchi, Elshenawy and Shaban in 2002, is an extension of the RSA scheme to the field of Gaussian integers using a modulus $N = PQ$ where P and Q are Gaussian primes such that $p = |P|$ and $q = |Q|$ are ordinary primes. The third cryptosystem [13], proposed by Castagnos in 2007, is a scheme over quadratic field quotients with an RSA modulus $N = pq$ based on Lucas sequences. In the three cryptosystems, the public key e and the private key d are linked by the equation

$$ed = 1 \pmod{(p^2-1)(q^2-1)}.$$

By using the continued fraction technique, Bunder, Nitaj, Susilo and Tonien [9] showed for the first time that the secret key can be recovered if $d^2e < 2N^3 - 18N^2$. In this chapter, we extend the work of [9]. We improve the bound to

$$d^2e < 2t\frac{(N^2 - \frac{5}{2}N)^2}{N+4t} \approx 2tN^3,$$

for an arbitrary parameter t, and the running time of our algorithm is $O(t \log N)$.

Our new attack is verified by an experiment with a 1024-bit modulus N, a 2029-bit public key e and a 520-bit private key d.

8.1 The Kuwakado-Koyama-Tsuruoka scheme

The Kuwakado-Koyama-Tsuruoka scheme [28] is a public-key cryptosystem based on elliptic curves

$$y^2 = x^3 + bx^2 \pmod{N}$$

over a ring $\mathbb{Z}_N$ where $N = pq$ is an RSA-modulus.

In this cryptosystem, plaintexts and ciphertexts are represented as points $P = (x, y)$ of the curve and the correctness of the algorithm is based on the equation

$$(p^2 - 1)(q^2 - 1)P = \mathcal{O}_N,$$

where $\mathcal{O}_N$ – the point at infinity – is the additive identity of the curve.

The scheme can be summarised as follows.

Key Generation:

- Choose two distinct prime numbers p and q of similar bit-lengths.
- Compute $N = pq$.
- Choose $e \in (1, (p^2 - 1)(q^2 - 1))$ such that $\gcd(e, (p^2 - 1)(q^2 - 1)) = 1$ and calculate

$$d = e^{-1} \pmod{(p^2 - 1)(q^2 - 1)} \in (1, (p^2 - 1)(q^2 - 1)).$$

- The public key is (N, e). The private key is (p, q, d).

Encrypt function:

- For a plaintext $m = (m_x, m_y) \in \mathbb{Z}_N \times \mathbb{Z}_N$, the ciphertext $c = (c_x, c_y) \in \mathbb{Z}_N \times \mathbb{Z}_N$ is determined as
  - Calculate
$$b = \frac{m_y^2 - m_x^3}{m_x^2} \pmod{N},$$
    this makes (m_x, m_y) a point on the curve $y^2 = x^3 + bx^2 \pmod{N}$,
  - On the curve $y^2 = x^3 + bx^2 \pmod{N}$, calculate the point

$$(c_x, c_y) = e(m_x, m_y).$$

Decrypt function:

- For a ciphertext $c = (c_x, c_y) \in \mathbb{Z}_N \times \mathbb{Z}_N$, the plaintext $m = (m_x, m_y) \in \mathbb{Z}_N \times \mathbb{Z}_N$ is determined as
  - Calculate
    $$b = \frac{c_y^2 - c_x^3}{c_x^2} \pmod{N},$$
    this makes (c_x, c_y) a point on the curve $y^2 = x^3 + bx^2 \pmod{N}$,
  - On the curve $y^2 = x^3 + bx^2 \pmod{N}$, calculate the point
    $$(m_x, m_y) = d(c_x, c_y).$$

8.2 The Elkamchouchi-Elshenawy-Shaban scheme

The Elkamchouchi-Elshenawy-Shaban scheme [18] is an extension of the RSA scheme over the domain of Gaussian integers. A Gaussian integer is a complex number of the form $a + bi$ where $a, b \in \mathbb{Z}$. The set of all Gaussian integers is the ring $\mathbb{Z}[i]$. The norm of a Gaussian integer $a + bi$ is $|a + bi| = a^2 + b^2$. A Gaussian prime is a Gaussian integer which is divisible only by a unit. The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$ and have norm 1. If $a^2 + b^2$ is a prime number in $\mathbb{Z}$, then $a + ib$ is a Gaussian prime. And if $p \in \mathbb{Z}$ is an ordinary prime number, then Gaussian integers p and pi are Gaussian primes if and only if $p \equiv 3 \pmod{4}$.

If P and Q are Gaussian primes and $N = PQ$, then for any Gaussian integer $\alpha \neq 0 \pmod{N}$, we have

$$\alpha^{(|P|-1)(|Q|-1)} = 1 \pmod{N}. \tag{8.1}$$

In the Elkamchouchi-Elshenawy-Shaban scheme, we use two large integers p and q which are Gaussian primes. So in this case, the equation (8.1) becomes

$$\alpha^{(p^2-1)(q^2-1)} = 1 \pmod{N}.$$

The scheme can be summarised as follows.

Key Generation:

- Choose two distinct prime numbers p and q of similar bit-lengths which are Gaussian primes.
- Compute $N = pq$.

- Choose $e \in (1, (p^2-1)(q^2-1))$ such that $\gcd(e, (p^2-1)(q^2-1)) = 1$ and calculate

$$d = e^{-1} \pmod{(p^2-1)(q^2-1)} \in (1, (p^2-1)(q^2-1)).$$

- The public key is (N, e). The private key is (p, q, d).

Encrypt function:

- For a plaintext $m \in \mathbb{Z}[i]$, the ciphertext $c \in \mathbb{Z}[i]$ is determined as

$$c = m^e \pmod{N}.$$

Decrypt function:

- For a ciphertext $c \in \mathbb{Z}[i]$, the plaintext $m \in \mathbb{Z}[i]$ is determined as

$$m = c^d \pmod{N}$$

8.3 The Castagnos scheme

The Castagnos scheme [13] is a public-key cryptosystem based on certain Lucas sequences. Let r be an integer. Define the sequence as follows

$$V_0(r) = 2, \quad V_1(r) = r, \quad V_{k+2}(r) = rV_{k+1}(r) - V_k(r).$$

The scheme can be summarised as follows.

Key Generation:

- Choose two distinct prime numbers p and q of similar bit-lengths.
- Compute $N = pq$.
- Choose $e \in (1, (p^2-1)(q^2-1))$ such that $\gcd(e, (p^2-1)(q^2-1)) = 1$ and calculate

$$d = e^{-1} \pmod{(p^2-1)(q^2-1)} \in (1, (p^2-1)(q^2-1)).$$

- The public key is (N, e). The private key is (p, q, d).

Encrypt function:

- For a plaintext $m \in \mathbb{Z}_N$, the ciphertext $c \in \mathbb{Z}_{N^2}$ is determined as
  - Choose a random integer $r \in \{1, 2, \ldots, N-1\} \setminus \{2, N-2\}$.
  - Calculate
$$c = (1 + mN)V_e(r) \pmod{N^2}.$$

Decrypt function:

- Precomputation:
$$\begin{aligned} d_{(p,1)} &= e^{-1} \pmod{(p-1)} \\ d_{(p,-1)} &= e^{-1} \pmod{(p+1)} \\ d_{(q,1)} &= e^{-1} \pmod{(q-1)} \\ d_{(q,-1)} &= e^{-1} \pmod{(q+1)} \\ inv_q &= p^{-1} \pmod{q} \\ inv_p &= q^{-1} \pmod{p} \end{aligned}$$

- For a ciphertext $c \in \mathbb{Z}_{N^2}$, the plaintext $m \in \mathbb{Z}_N$ is determined as
  - Calculate
$$\begin{aligned} i_p &= (\frac{c^2-4}{p}), \text{ here } (\frac{x}{y}) \text{ denotes the Legendre symbol} \\ r_p &= V_{d_{(p,i_p)}}(c) \pmod{p} \\ i_q &= (\frac{c^2-4}{q}) \\ r_q &= V_{d_{(q,i_q)}}(c) \pmod{q} \\ r &= r_p + p(r_q - r_p)inv_q \pmod{N} \\ t_p &= c/V_e(r) \mod p^2 \\ s_p &= (t_p - 1)/p \\ m_p &= s_p \times inv_p \pmod{p} \\ t_q &= c/V_e(r) \mod q^2 \\ s_q &= (t_q - 1)/q \\ m_q &= s_q \times inv_q \pmod{q} \\ m &= m_p + p(m_q - m_p)inv_q \pmod{N}. \end{aligned}$$

The interested reader is referred to [13] for the correctness proof of the algorithm.

8.4 The new attack

In the three RSA-variant schemes considered in this chapter, the public key e and the private key d satisfy the equation

$$ed = 1 \pmod{(p^2-1)(q^2-1)}.$$

We now present our attack on the three schemes based on the continued fraction technique.

Theorem 8.4.1 *Let t be a fixed positive integer. If the following conditions are satisfied*

- $q < p < 2q$
- $0 < e, d < (p^2-1)(q^2-1)$
- $ed - k(p^2-1)(q^2-1) = 1$
- $\boxed{d^2 e < 2t\dfrac{(N^2 - \frac{5}{2}N)^2}{N+4t} \approx 2tN^3}$

and

$$N_i = N^2 + 1 - \frac{5}{2}N + (2i-1)\frac{N}{4t}, 1 \le i \le t,$$

then $\frac{k}{d}$ is a convergent of the regular continued fraction of $\frac{e}{N_i}$ for some $i \in [1,t]$ and there is an algorithm with time complexity $O(t\log(N))$ that can determine the secret information p, q, d, k from the public key (N, e).

Proof. It follows from $q < p < 2q$ that $1 < \frac{p}{q} < 2$, so since the function $f(x) = x + \frac{1}{x}$ is increasing on $[1, +\infty)$, we have

$$2 < \frac{p}{q} + \frac{q}{p} < 2 + \frac{1}{2} = \frac{5}{2}.$$

Therefore,

$$2N < p^2 + q^2 < \frac{5}{2}N$$

and

$$N^2 + 1 - 2N > (p^2-1)(q^2-1) > N^2 + 1 - \frac{5}{2}N.$$

Let

$$\phi_{min} = N^2 + 1 - \frac{5}{2}N, \quad \phi_{max} = N^2 + 1 - 2N \text{ and } \phi = (p^2-1)(q^2-1)$$

then $\phi \in (\phi_{min}, \phi_{max})$. From the definition of N_i, we can see that

$$N_i = \phi_{min} + (2i-1)\frac{\phi_{max} - \phi_{min}}{2t},$$

so by Lemma 7.3.1, there exists N_i such that

$$|\phi - N_i| \leq \frac{\phi_{max} - \phi_{min}}{2t}.$$

We have

$$\begin{aligned}
\left|\frac{e}{N_i} - \frac{k}{d}\right| &= \left|\left(\frac{e}{N_i} - \frac{e}{\phi}\right) + \left(\frac{e}{\phi} - \frac{k}{d}\right)\right| \\
&= \left|\frac{e(\phi - N_i)}{N_i\phi} + \frac{1}{d\phi}\right| \\
&= \left|\frac{e(\phi - N_i)}{N_i\phi} + \frac{e}{\phi(k\phi+1)}\right| \\
&\leq \frac{e|\phi - N_i|}{N_i\phi} + \frac{e}{\phi(k\phi+1)} \\
&\leq \frac{e\frac{\phi_{max}-\phi_{min}}{2t}}{\phi_{min}^2} + \frac{e}{\phi_{min}^2} = \frac{e(\phi_{max} - \phi_{min} + 2t)}{2t\phi_{min}^2} \\
&< \frac{e(\phi_{max} - \phi_{min} + 2t)}{2t(\phi_{min}-1)^2} = \frac{e}{2t}\frac{\frac{1}{2}N + 2t}{(N^2 - \frac{5}{2}N)^2} = \frac{e}{4t}\frac{N + 4t}{(N^2 - \frac{5}{2}N)^2} \\
&< \frac{1}{2d^2}.
\end{aligned}$$

Thus, by Theorem 1.4.9, $\frac{k}{d}$ is equal to a convergent of the regular continued fraction of $\frac{e}{N_i}$. So we need to go through the list of all convergents of $\frac{e}{N_i}$ for each $1 \leq i \leq t$ to determine the secret information p, q, d, k.

Given each convergent $c_n = \frac{p_n}{q_n}$ of $\frac{e}{N_i}$, by Theorem 1.4.4, $\gcd(p_n, q_n) = 1$. The equation $ed - k\phi = 1$ also implies $\gcd(k, d) = 1$. So if $\frac{k}{d} = \frac{p_n}{q_n}$ then $p_n = k$ and $q_n = d$. Based on the equation $ed - k\phi = 1$, it is easy to check if $p_n = k$ and $q_n = d$ or not as follows:

- Check if $eq_n - 1$ is divisible by p_n or not. If not then the convergent $c_n = \frac{p_n}{q_n} \neq \frac{k}{d}$.
- If so, calculate $\phi = \frac{eq_n - 1}{p_n}$
- Calculate $S = p^2 + q^2 = N^2 + 1 - \phi$
- Solving the quadratic equation $x^2 - Sx + N^2 = 0$ for $x_{1,2} = p^2, q^2$ and check if $\sqrt{x_1}$ and $\sqrt{x_2}$ are prime numbers.

Since there are t such numbers $\frac{e}{N_i}$ and each of these numbers $\frac{e}{N_i}$ has $O(\log N)$ convergents, so the algorithm runs with time complexity $O(t \log N)$. ■

8.5 An experimental result

We consider two RSA primes p and q, both of 512 bits, which give us a 1024-bit modulus N. The public exponent e is 2029-bit and the secret exponent d is 520-bit.

$$
\begin{aligned}
p = &1009926345\ 7471330007\ 1984329453\ 1837129144\ 5329854502 \\
&1579205949\ 1972427206\ 6832404994\ 0387919056\ 4150845276 \\
&8065924106\ 7922890816\ 2666245720\ 1616730699\ 1117239731\ 85481 \\
q = &9201052432\ 2086390067\ 1386866266\ 0639973895\ 0237269245 \\
&6878261382\ 5773843108\ 2681621528\ 1513707044\ 8098390827 \\
&1161420676\ 8781444754\ 1784724352\ 5840645389\ 7707377855\ 3491 \\
N = &9292385259\ 8882409829\ 3162082225\ 5290648240\ 2932610895 \\
&2796745930\ 4569281602\ 2535261774\ 6000624542\ 0686015350 \\
&5820019086\ 9644402726\ 0931963319\ 2462241182\ 6579351302 \\
&0782053736\ 0725528276\ 5503973157\ 0642939798\ 0805113181 \\
&1631153462\ 5580255681\ 0453116780\ 9138251914\ 8143650220 \\
&1487534725\ 1944638440\ 3016589748\ 5133626528\ 3338290596\ 23064171
\end{aligned}
$$

e =5610945328 2671796041 5829077437 9519142056 5955456458
7016831195 6891736518 8405496534 0274145492 4223492328
5533946739 3132613402 2802793166 8707714667 2017196874
2057028761 3007844191 6424007923 8588782842 5888389498
2399842002 8312226377 0538147674 6869931106 0864836776
4239757895 9256035850 8693271128 6691302868 6894236736
3858899449 4578621026 8249617044 5653141105 6506148300
2531330952 9779988125 0306197976 3903833872 8515848925
1679290735 1472231296 9415530850 4617614777 4425005468
7389111903 1488774848 5654348435 7158394635 1774298241
7614264452 0801690300 4327479471 1402065512 8418504644
3456306876 4694318782 5003370247 1823625867 3480338561 6726117398 7

We use $t = 1$ and found $\frac{k}{d}$ at the 306th convergent of $\frac{e}{N_1} = \frac{e}{N^2 - \frac{9}{4}N + 1}$

k =2230382597 4699469998 8596682209 1052908389 5670986870
3180114419 9709650127 6686575639 3075936836 3045074562
2035858758 0823897378 9584493028 0368787713 7164782033 05
d =3432398830 0653048574 9095039954 0696608634 7176500716
5270469723 1729592771 5916988280 2606127982 0330727277
4886481556 9574042901 8560993999 8583219062 8701414555 7262923

Bibliography

[1] M. Abramowitz and I. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. National Bureau of Standards, 1964.

[2] E. Bach and J. Shallit, *Algorithmic number theory, Volume I: Efficient algorithms*. MIT Press, 1996.

[3] A. Beardon and I. Short, "The Seidel, Stern, Stolz and Van Vleck theorems on continued fractions," *Bulletin of the London Mathematical Society*, vol. 42, pp. 457–466, 2010.

[4] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, 1986.

[5] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," *IEEE Transactions on Information Theory*, vol. 46, pp. 1339–1349, 2000.

[6] J. M. Borwein, A. J. van der Poorten, J. O. Shallit, and W. Zudilin, *Neverending fractions: An introduction to continued fractions*. Cambridge University Press, 2014.

[7] C. Brezinski, *History of continued fractions and Padé approximants*. Springer-Verlag, 1991.

[8] M. Bunder, P. Nickolas, and J. Tonien, "On the harmonic continued fractions," submitted.

[9] M. Bunder, A. Nitaj, W. Susilo, and J. Tonien, "A new attack on three variants of the RSA cryptosystem," in *Proceedings of the 21st Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science 9723*, 2016, pp. 258–268.

[10] M. Bunder and J. Tonien, "A new improved attack on RSA," in *Proceedings of the 5th International Cryptology and Information Security Conference*, 2016, pp. 101–110.

[11] ——, "A new attack on the RSA cryptosystem based on continued fractions," *Malaysian Journal of Mathematical Sciences*, vol. 11, no. S3, pp. 45–57, 2017.

[12] ——, "Closed form expressions for two harmonic continued fractions," *The Mathematical Gazette*, vol. 101, no. 552, pp. 439–448, 2017.

[13] G. Castagnos, "An efficient probabilistic public-key cryptosystem over quadratic field quotients," *Finite Fields and Their Applications*, vol. 13, pp. 563–576, 2007.

[14] W. Y. C. Chen, A. M. Fu, and I. F. Zhang, "Faulhaber's theorem on power sums," *Discrete Mathematics*, vol. 309, pp. 2974–2981, 2009.

[15] H. Cohn, "A short proof of the simple continued fraction expansion of e," *American Mathematical Monthly*, vol. 113, pp. 57–62, 2006.

[16] J. B. Conway, *Functions of one complex variable*. Springer, 1978, vol. 1.

[17] H. S. M. Coxeter, "Frieze patterns," *Acta Arithmetica*, vol. 18, pp. 297–310, 1971.

[18] H. Elkamchouchi, K. Elshenawy, and H. Shaban, "Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers," in *Proceedings of the 8th International Conference on Communication Systems*, 2002, pp. 91–95.

[19] L. Euler, "De fractionibus continuis dissertatio," *Commentarii academiae scientiarum imperialis Petropolitanae*, vol. 9, pp. 98–137, 1744.

[20] ——, "De fractionibus continuis observationes," *Commentarii academiae scientiarum imperialis Petropolitanae*, vol. 11, pp. 32–81, 1750.

[21] G. Hardy and E. Wright, *An introduction to the theory of numbers*, 6th ed. Oxford University Press, 2008.

[22] C. Hermite, "Sur la fonction exponentielle," *Comptes rendus de l'Académie des sciences Paris*, pp. 18–24, 74–79, 226–233, 285–293, 1873.

[23] W. B. Jones and W. J. Thron, *Continued fractions: Analytic theory and applications*. Reading, Massachusetts: Addison-Wesley, 1980.

[24] A. M. Kane, "On the use of continued fractions for stream ciphers," in *Proceedings of the 2009 International Conference on Security & Management*, 2009, pp. 583–589.

[25] A. N. Khovanski, *The application of continued fractions and their generalizations to problems in approximation theory*. Groningen: P. Noordhoff, 1963.

[26] S. Khrushchev, "On Euler's differential methods for continued fractions," *Electronic Transactions on Numerical Analysis*, vol. 25, pp. 178–200, 2006.

[27] D. E. Knuth, *The art of computer programming*, 3rd ed. Addison-Wesley, 1998, vol. 2.

[28] H. Kuwakado, K. Koyama, and Y. Tsuruoka, "A new RSA-type scheme based on singular cubic curves $y^2 = x^3 + bx^2 \pmod{n}$," *IEICE Transactions on Fundamentals*, vol. E78-A, pp. 27–33, 1995.

[29] A.-M. Legendre, *Essai sur la théorie des nombres*. Duprat, Paris, An VI, 1798.

[30] L. Lorentzen and H. Waadeland, *Continued fractions, Volume 1, Convergence theory*. Atlantis Press, 2008.

[31] D. I. Nassr, H. M. Bahig, A. Bhery, and S. S. Daoud, "A new RSA vulnerability using continued fractions," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications AICCSA 2008*, 2008, pp. 694–701.

[32] I. Niven, "Formal power series," *American Mathematical Monthly*, vol. 76, pp. 871–889, 1969.

[33] C. D. Olds, *Continued fractions*. Washington: Mathematical Association of America, 1963.

[34] ——, "The simple continued fraction expansion of e," *American Mathematical Monthly*, vol. 77, pp. 968–974, 1970.

[35] T. J. Osler, "A proof of the continued fraction expansion of $e^{1/M}$," *American Mathematical Monthly*, vol. 113, pp. 62–66, 2006.

[36] T. J. Pickett and A. Coleman, "Another continued fraction for π," *American Mathematical Monthly*, vol. 115, pp. 930–933, 2008.

[37] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[38] L. Seidel, *Untersuchungen über die Konvergenz und Divergenz der Kettenbrüche*, Habilschrift München, 1846.

[39] M. A. Stern, "Über die Kennzeichen der Konvergenz eines Kettenbruchs," *Journal für die Reine und Angewandte Mathematik*, vol. 37, pp. 255–272, 1848.

[40] J. Tonien, "New year identity," *Mathematics Magazine*, vol. 87, no. 5, p. 337, 2014.

[41] ——, "A simple proof of Euler's continued fraction of $e^{1/M}$," *The Mathematical Gazette*, vol. 100, no. 548, pp. 279–287, 2016.

[42] ——, "A continued fraction inspired by an identity of Euler," *The Mathematical Gazette*, vol. 101, no. 550, pp. 115–121, 2017.

[43] ——, "A new elementary proof of Euler's continued fractions," *The Mathematical Gazette*, vol. 102, no. 553, pp. 105–111, 2018.

[44] A. V. Ustinov, "Geometric proof of Rødseth's formula for Frobenius numbers," *Proceedings of the Steklov Institute of Mathematics*, vol. 276, pp. 275–282, 2012.

[45] J. Wallis, *Arithmetica infinitorum*. 1656, English translation: J.A. Stedall, The arithmetic of infinitesimals: John Wallis, 1656, Springer, 2004.

[46] M. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, vol. 36, pp. 553–558, 1990.